all rights reversed

∇HACKER

Season 05 / Issue 10

τεύχος 058 - Airborne Edition

Το προσωπικό σας Dropbox με το Raspberry Pi [*]

Τα virtual hosts του Apache

Ευέλικτο storage box για το VPS σας

Πλήρες LEMP stack για έναν Leap server

deltaCast s03e05 | Linux 4SuperUsers [μέρος 5]

Let's Encrypt certificate, για τον Apache στο openSUSE

Πώς θα έχετε τον πιο πρόσφατο Linux kernel στο Leap 42.2

[*] και ό,τι πρέπει να γνωρίζετε για να αγαπήσετε το Nextcloud

all rights reversed

HACKER


CMYK & WEB
cmykandweb.gr
GRAPHIC DESIGN
design • layout • web

#dH058 | Περιεχόμενα

Εκδότης / Διευθυντής	Χρήστος Βαρελάς
Αρχισυντάκτης	Παναγιώτης Βαρελάς
Σύμβουλοι έκδοσης	Βούλα Παυλίδου
Σύνταξη	Παναγιώτης Βαρελάς, Χρήστος Βαρελάς, Πάνος Γεωργιάδης, Γιώργος Γιάννου, Γιάννης Κρομμύδας, Πέτρος Κυλαδίτης, Μέσος Παπαδόπουλος (TM), Χρίστος Τόμπρας, @arkoudos
Γραμματική επιμέλεια	Βούλα Παυλίδου
Καλλιτεχνική Επιμέλεια	Πέτρος Φιλιππίδης

Το ψηφιακό περιοδικό deltaHacker είναι συνδρομητικό και εκδίδεται από την Parabing Creations. Ο δικτυακός τόπος του περιοδικού είναι στο https://deltahacker.gr και το email επικοινωνίας είναι το talk2us@deltahacker.gr. Οι γενικές πληροφορίες για τις συνδρομές παρατίθενται στο https://deltahacker.gr/order κι από την ίδια σελίδα γίνονται οι παραγγελίες.

Ό,τι σας αρέσει, σχεδόν πάντα

του Χρήστου Βαρελά

Φίλες και φίλοι,

- Πάντα πιστεύαμε, πιστεύουμε και θα συνεχίσουμε να πιστεύουμε, ότι ο Σύγχρονος Άνθρωπος™ οφείλει να επιδιώκει και να κάνει ό,τι του αρέσει.
- Αρκεί βεβαίως αυτό που του αρέσει να μη βλάπτει τους συνανθρώπους του, οπότε αμέσως αμέσως αποκλείουμε κατηγορίες δραστηριοτήτων τις οποίες νομίζουμε πως δεν έχει νόημα ούτε καν ν' αναφέρουμε.
- Άλλωστε μεγάλα παιδιά είμαστε – και καταλαβαινόμαστε.
- Κι επειδή είμαστε μεγάλα παιδιά (και καταλαβαινόμαστε), δεν χρειάζεται να σημειώσουμε ότι μερικές φορές *δεν* μπορούμε να κάνουμε ό,τι θέλουμε. Τι να γίνει, δεν είμαστε μόνοι μας στον Πλανήτη και συχνά υποχρεωνόμαστε να κάνουμε πράγματα που δεν μας πολυαρέσουν.
- Αλλά όταν τελειώνουμε με τις όχι-και-τόσο ευχάριστες ή ακόμη και δυσάρεστες εργασίες και υποθέσεις, αξίζει να επικεντρωνόμαστε ξανά σε ό,τι μας έλκει κι έχει κάτι να μας πει.
- Το αποτέλεσμα είναι ότι, μέσω ευχάριστων για εμάς ενασχολήσεων, διαρκώς γινόμαστε καλύτεροι κι ωφελούμαστε. Και δεν ωφελούμαστε μόνον εμείς, αλλά συνήθως ωφελούνται και οι γύρω μας. Σκεφτείτε: Ενώ το κίνητρό μας είναι καθαρά εγωιστικό (κάνω αυτό που *μου* αρέσει), τελικά κερδίζουν περισσότεροι από ένας άνθρωποι.
- Έχουμε μια ροπή προς τη γενικολογία, φίλες και φίλοι, και φαίνεται. Αυτή τη φορά όμως αξίζει να γίνουμε λίγο πιο συγκεκριμένοι, αναφέροντας ένα ή δύο παραδείγματα.
- Στο πρώτο παράδειγμα συζητάμε για έναν αρθρογράφο που δουλεύει σε ψηφιακό περιοδικό τεχνολογίας. Αλήθεια, γιατί κάποιος θα ήθελε να ασχοληθεί με το αντικείμενο; Η προφανής απάντηση είναι διότι (σχεδόν) όλοι μας κάτι πρέπει να κάνουμε για να ζήσουμε. Έτσι είναι – κι άνετα μπορούμε να φανταστούμε έναν αρθρογράφο ο οποίος ξεκίνησε να κάνει αυτή τη δουλειά μόνο και μόνο επειδή έπρεπε να εργαστεί. Ίσως όμως υπήρχαν κι άλλοι λόγοι που οδήγησαν το φίλο μας εκεί

που είναι κι όχι, π.χ., στον πολλά υποσχόμενο κλάδο του αγροτουρισμού (λέμε τώρα) ή στον ακόμα πιο πολλά υποσχόμενο κλάδο της μεσογειακής ιχθυοκαλλιέργειας (σκοτοδίνη).

- Ίσως του αρέσει η τεχνολογία (μάλλον σίγουρο) κι έχει έφεση προς τον γραπτό λόγο (πολύ πιθανό). Επιπρόσθετα μάλλον του αρέσει και η έρευνα, διασκεδάζει δοκιμάζοντας/χαλώντας/φτιάχνοντας και, last but not least, καταφέρνει και μεταδίδει τις όποιες γνώσεις έχει ακόμη και σε αναγνώστες οι οποίοι δεν είχαν καν ακούσει για το εκάστοτε θέμα που παρουσιάζει κι αναπτύσσει.
- Θα συμφωνήσετε, φανταζόμαστε, ότι ο υποθετικός αυτός αρθρογράφος τεχνολογίας βρίσκεται στο σωστό χώρο και μάλιστα πληρώνεται *χωρίς* να δουλεύει. Ναι, σωστά διαβάσατε: δεν δουλεύει ο άνθρωπος, αφού ό,τι κάνει το βλέπει πρώτα σαν διασκέδαση και μετά ως οτιδήποτε άλλο.
- Αν τώρα θέλουμε να είμαστε λίγο περισσότερο ακριβολόγοι και προσγειωμένοι στην πραγματικότητα, πρέπει στο σημείο αυτό να επισημάνουμε ότι ο φίλος μας δεν κάνει πάντα ό,τι του αρέσει. Συχνά αναγκάζεται και δουλεύει με άλλους συναδέλφους κι όλοι μαζί τεστάρουν κι αξιολογούν φορητά media players (μιλάμε για *το* blast from the past), φωτογραφικούς εκτυπωτές (δάκρυα από τη βαρεμάρα) ή ακόμη και πολυσυσκευές που συνδυάζουν εκτυπωτή, σαρωτή και φαξ (αντίο κόσμε).
- Γενικά όμως του αρέσει πολύ η δουλειά του και, όπως μπορείτε να υποθέσετε, αυτό τον κάνει να είναι καλός και μεταξύ άλλων να απολαμβάνει και μια κάποια εργασιακή ασφάλεια. Ποιοι άλλοι κερδίζουν, εκτός από εκείνον; Πρώτα πρώτα κερδίζουν οι άνθρωποι του οικογενειακού του περιβάλλοντος, για προφανείς μάλλον λόγους. Κερδίζουν όμως και αναγνώστες του περιοδικού. Κατ' αρχάς, είναι αποδέκτες *και* της καλής δουλειάς του αρθρογράφου και χαίρονται με ό,τι διαβάζουν. Κατά δεύτερον, ίσως μαθαίνουν πράγματα που τους είναι άμεσα χρήσιμα. Επιπρόσθετα, κάποιοι από τους αναγνώστες εμπνέονται και προχωρούν σε συγκεκριμένες επιλογές, π.χ., περί σπουδών ή επαγγελματικού προσανατολισμού. Αρκετοί λοιπόν ωφελούνται, στον έναν ή στον άλλον βαθμό, από τα αποτελέσματα της εργασίας ενός ανθρώπου, ο οποίος αγαπά αυτό που κάνει. Ο ίδιος βέβαια δεν είναι δυνατόν να γνωρίζει για τα αποτελέσματα της δουλειάς του – και μάλλον αδιαφορεί. Σημασία για εκείνον έχει να κάνει ό,τι του αρέσει.
- Στο δεύτερο παράδειγμά μας, ας συζητήσουμε για έναν άλλον φίλο ο οποίος δουλεύει ως Quality Assurance Engineer σε μια εταιρεία που παρέχει υποστήριξη σε Open Source Software. Με λίγα λόγια –κι επειδή

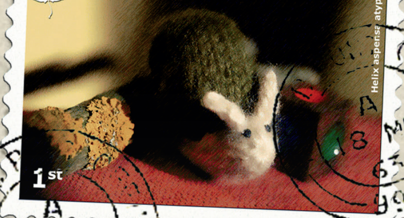
δεν χρειάζεται να είμαστε 100% ακριβείς για το job description–, ας πούμε ότι κάθε φορά που εφαρμόζονται patches σε λογισμικό που υποστηρίζει η εταιρεία τότε ο άνθρωπός μας οφείλει να βεβαιώνει ότι το αναβαθμισμένο λογισμικό δουλεύει σωστά κι όπως προβλέπεται. Οι πελάτες, δηλαδή, με κανέναν τρόπο δεν πρέπει να παίρνουν λογισμικό κατώτερης ποιότητας, σε σχέση με εκδόσεις που ήδη χρησιμοποιούσαν.

- Επαναλαμβάνουμε το ερώτημα που θέσαμε προηγουμένως: Γιατί κάποιος θα ήθελε να δουλέψει ως QA Engineer; Ο προφανής λόγος είναι διότι χρειάζεται μια δουλειά για να ζήσει και μπορούμε να φανταστούμε έναν QA Engineer ο οποίος ξεκίνησε στο χώρο μόνο και μόνο επειδή *πρέπει* να δουλέψει κ.λπ. κ.λπ. Ίσως όμως υπάρχουν κι άλλοι λόγοι που οδήγησαν το (νέο) φίλο μας εκεί που τώρα είναι κι όχι, π.χ., στο να γίνει ψυκτικός (ξέρετε πόσα βγάζουν οι καλοί ψυκτικοί;) ή στο να χτίσει καριέρα ως stand up comedian (τιμή, δόξα και χρήμα, για τους πετυχημένους κωμικούς του είδους).
- Ίσως του αρέσει το Linux ειδικότερα και το F/LOSS γενικότερα. Μπορεί επίσης να έχει έφεση προς την αναλυτική προσέγγιση στην επίλυση προβλημάτων και να γοητεύεται από τον προγραμματισμό, χωρίς να είναι developer. Επειδή εξάλλου βαριέται ν' ασχολείται με το ίδιο πράγμα ξανά και ξανά, όταν συνειδητοποίησε πως δεν θα κάνει QA μόνο για μία εφαρμογή τότε είδε μπροστά του ν' ανάβει ένα πράσινο φως.
- Ο φίλος μας δεν τα πάει άσχημα με το QA (ακόμα μαθαίνει) κι αυτό βεβαίως είναι καλό για τον ίδιο. Είναι φυσικά καλό και για τους συναδέλφους του, άρα και για την εταιρεία. Οι δε πελάτες δεν ανακαλύπτουν regressions (ας το ελπίσουμε!) στις ανανεωμένες εκδόσεις του λογισμικού που λαμβάνουν, επομένως όλα δείχνουν όμορφα κι ωραία και κανείς δεν παραπονιέται.
- Ποιοι άλλοι ωφελούνται απ' αυτή την κατάσταση; Όπως και στο προηγούμενο παράδειγμα, η προφανής απάντηση δείχνει στο οικογενειακό περιβάλλον του μηχανικού (είμαστε έτοιμοι να τον πούμε "κιού-έι", δειλιάσαμε όμως). Μάλιστα. Κανείς άλλος, ωφελείται; Χμ, ίσως. Αν, π.χ., υποθέσουμε ότι ο φίλος μας (ο κιού-έι) τα πηγαίνει καλά με τον γραπτό λόγο, τότε δεν είναι διόλου απίθανο να υποθέσουμε κι ότι μπλογκάρει για τη δουλειά του, για τις νέες τεχνολογίες που μελετά αλλά και για τα ενδιαφέροντα προβλήματα που αντιμετωπίζει. Ίσως μάλιστα να μη γράφει σε μπλογκ που το διαβάζουν 5-6 άνθρωποι, αλλά σε (ψηφιακό) περιοδικό με λίγους περισσότερους συνδρομητές. Θα μπορούσαμε εδώ να σκεφτούμε ότι το πρόσωπο

του πρώτου παραδείγματος είναι ίδιο με το πρόσωπο του δεύτερου παραδείγματος, απλά σε διαφορετικές χρονικές περιόδους. Πραγματικά όμως, δεν υπάρχει λόγος για τόσο τραβηγμένα σενάρια.

- Φανταστείτε ότι το πρόσωπο του δευτέρου παραδείγματος (το οποίο σχεδόν σίγουρα είναι διαφορετικό από εκείνο του πρώτου παραδείγματος) έχει να δουλέψει με ένα προϊόν storage που βασίζεται στο Ceph και η εταιρεία πουλά υποστήριξη σε όσους ενδιαφέρονται να το αξιοποιούν. Ο φίλος μας τότε θα ξεκινήσει μαθαίνοντας γι' αυτό το Ceph, για τα storage clusters, για τα διαφορετικά interfaces (object/block/file-level) που παρέχει μια τέτοια πλατφόρμα στις εφαρμογές κ.ο.κ. Μετά θα θελήσει να υλοποιήσει τα δικά του storage clusters για testing, τα οποία μάλιστα δεν είναι υποχρεωτικό να βασίζονται σε physical hardware (ακόμη κι ένα laptop με 16GB RAM είναι αρκετό για ένα απλό cluster εκπαιδευτικού χαρακτήρα). Αν κάποια στιγμή στιγμή ξεκινήσει να γράφει άρθρα για το όλο θέμα, ώστε να έχει τις νεοαποκτηθείσες γνώσεις και μεθοδολογίες σε μια καλή σειρά και να μη χάνεται, δεν θα κερδίσουν κάτι και μερικοί απ' όσους τα διαβάσουν; Δεν ξέρουμε πώς το βλέπετε εσείς, σκεφτόμαστε όμως ότι δυο-τρεις άνθρωποι, τους οποίους ο φίλος μας δεν γνωρίζει καν, όλο και κάτι θα μάθουν κι αργά ή γρήγορα θα τους φανεί χρήσιμο.
- Τι καθιστά μη-μηδενική την πιθανότητα για θετικά αποτελέσματα, στα δύο μόλις από τα ατέλειωτα σενάρια που θα μπορούσαμε να φανταστούμε; Μα, το γεγονός ότι οι πρωταγωνιστές τους φροντίζουν και κάνουν ό,τι τους αρέσει.
- Σχεδόν πάντα, φυσικά.

ΥΓ. *Οποιαδήποτε ομοιότητα με πρόσωπα και καταστάσεις του πραγματικού κόσμου είναι εντελώς συμπτωματική – εκτός από τις περιπτώσεις που δεν είναι.*





Ουέλ, μέλ

Αγαπητοί μου,

Καλοκαίριασε.

Τρόπος του λέγειν δηλαδή, γιατί εδώ που είμαστε καθισμένοι, στην αποβάθρα του Χένινγκσβερ, στα νησιά Λόφοτεν, κάνει τέτοιο ψοφόκρυο που αναρωτιέται κανείς πώς και συνεχίζουν να κατοικούνται τέτοια μέρη.

Έχει βέβαια ήλιο, δε λέω, αλλά το βουνό που βλέπω μπροστά μου έχει χιόνια.

Υπερβάλλω βέβαια. Χιόνια έχει, αλλά βουνό, δεν θα το έλεγες. Λόφοτεν όνομα και πράμα. Ένα λοφάκι κακοτράχαλο, κάτι σαν τα Τουρκοβούνια αλλά στο πιο νορβηγικό. Πάνω από διακόσια μέτρα ύψος δεν το κόβω.

Περιμένουμε το φέρυ που θα μας περάσει απέναντι. Μετά θα πάρουμε το λεωφορείο για Μπγιέρκβικ, από όπου με ανταπόκριση θα πάρουμε το λεωφορείο για Τρόμσο. Από Τρόμσο πετάμε για Ίναρι, στην Φινλανδική Λαπωνία. Στόχος μας είναι να είμαστε στο Ίναρι ίσα πριν βραδιάσει, για να προλάβουμε (αν μπορέσουμε) τις εορταστικές εκδηλώσεις του Vappu. Vappu, όπως εύκολα μπορεί ο καθείς να βρει στον ιντερνέ, ονομάζουν οι Φινλανδοί την Πρωτομαγιά.

Το Vappu, όπως προκύπτει αβίαστα από τα δεδομένα, πέφτει την Πρωτομαγιά. Ο χρόνος μας λοιπόν είναι λίγο τσίμα τσίμα.

Το πρόβλημα με τη Σκανδιναβία είναι πως κοιτάς στον χάρτη και όλα μοιάζουν να είναι το ένα δίπλα στο άλλο. Ε, ένα καραβάκι είναι, λες, θα το πάρουμε. Και μετά συνειδητοποιείς πως το ταξίδι με το «καραβάκι», από το ένα χωριό στο άλλο, κρατάει ξέρω 'γω 32 ώρες. Ή, εναλλακτικώς, μία ώρα και 45 λεπτά με το αεροπλάνο.

Χαμός.

Λέμε λοιπόν ότι θέλουμε να προλάβουμε το Vappu, αλλά, μεταξύ μας, χλωμό το βλέπω. Κατά τα άλλα έχουμε ήδη αγοράσει και φοράμε τα παραδοσιακά πρωτομαγιάτικα κασκετάκια του Vappu. Είμεθα μια παρέα καθ' όλα αυθεντικών ντόπιων περιηγητών.

Προς το παρόν περιηγούμαστε περιμένοντας στην αποβάθρα.

Έχουμε καιρό να τα πούμε και αναρωτιόμουν, να πω την αλήθεια, τι να σας γράψω. Μου είναι προφανές πως δεν περιμένετε από εμένα για να ενημερωθείτε περί όσων γραφικών λαμβάνουν χώρα στη γαλανή μας πατρίδα. Υποθέτω, μάλιστα, πως θα έχετε ενημερωθεί και για τα πιο βασικά σημεία της πρόσφατης διεθνούς επικαιρότητας.

Γιου νόου, Τραμπ; Λεπέν; Μπρέξιτ;

Εντάξει, τη Λεπέν δεν την είδαμε ακόμα, αλλά εδώ που σας γράφω, παραμονές του Vappu στην Νορβηγική Λαπωνία, σας γράφω με το βλέμμα στο μέλλον.

Μηδένα προ του τέλους, αγαπητοί μου. Από τη στιγμή που καταλήξαμε συμφιλιωμένοι με την ιδέα ότι περνάει η Λεπέν στο δεύτερο γύρο, δεν νομίζω πως θα ξεμπλέξουμε εύκολα.

Σας το έλεγα και πιο παλιά, με την αφορμή των Αβγών. This is not going to end up well.

Τέλος πάντων.

Η εξαδέλφη έχει βρει και ξεφυλλίζει μια Νορβηγική εφημερίδα. Πρωτοσέλιδο έχει τον Τραμπ. Δίπλα του, ένθετη φωτό, ο Κιμ Γιονγκ Ουν.

Στρέφω το βλέμμα αλλού. Τραμπ; Ποιος είναι ο Τραμπ; Νορβηγός είναι; Με τέτοιο μαλλί; Μήπως του ΟΗΕ; Μήπως απ' την Βόρειο Κορέα; Θα τον θυμόμουν.

Τα Νορβηγικά μου χρειάζονται λίγο ξεσκόνισμα. Δεν καταλαβαίνω. Τον αγνοώ.

Κοιτάζω αλλού.

Δεν τον αγνοώ καθόλου βέβαια.

Υπό άλλας συνθήκας ναι, θα τον αγνοούσα. Η το πολύ πολύ να τον σχολίαζα λίγο για να κάνουμε πλάκα: Καροτί φράντζα, ξεχειλωμένο σακάκι, περίεργος μορφασμός, τα γνωστά.

Όμως, αγαπητοί μου, το πράγμα με τον Τραμπ είναι πολύ σοβαρό. Δεν μιλάω με όρους πολιτικής ή άλλης διαφωνίας. Το πρόβλημα δεν έχει να κάνει με το τείχος που θα προστατέψει το Μεξικό ή με το ότι οι πλούσιοι θα πληρώνουν πλέον λιγότερους φόρους. Μεγάλα παιδιά είναι εκεί στην Αμερική, αυτά είναι θέματα προς συζήτηση. Θα διαφωνήσουνε, θα μαλώσουνε, θα ψηφίσουνε, κάποια άκρη θα βγει.

Με τον Τραμπ μιλάμε για κάτι πολύ πιο σοβαρό (και επικίνδυνο).

Θα θυμάστε ίσως τι έγινε με την τελετή ορκωμοσίας του. Τα υπέροχα πλήθη (not). Ο ενθουσιασμός. Και στη μέση αυτός. Ακίνητος. Περήφανος. Βράχος. Βγαίνει η εκπρόσωπός του, αγαλλιασμένη. Η μεγαλύτερη συγκέντρωση κόσμου σε τελετή ορκωμοσίας, κ.λπ. κ.λπ.

Τι λέτε καλέ κυρία; Θα μας τρελάνετε; Τρεις κι ο κούκος ήτανε, το δείχνουν και οι φωτογραφίες. Δεν τις είδατε;

Ε, λοιπόν όχι. Ακλόνητη η κυρία. Απερίσπαστος και ο Τραμπ. Ευθυτενής. Δεν έχει σημασία τι δείχνουν οι φωτογραφίες σας. Δεν έχει σημασία τι λένε τα δικά σας γεγονότα. Εμείς έχουμε άλλα γεγονότα. Δικά μας. Καλύτερα. Εναλλακτικά. Alternative.

Με αφορμή τον Τραμπ όλοι πλέον έχουμε βρεθεί να μιλάμε για fake news, post truths, alternative facts. Μιλάμε και γελάμε.

Γελάμε, αλλά το πράγμα είναι σοβαρό.

Ο Τράμπ δεν είναι ο γραφικός του καφενείου που λέει και καμιά παπαριά να περάσει η ώρα.

Το πρόβλημα δεν είναι καν ότι ο Τραμπ λέει ψέματα όπως, ξέρω γω, τόσοι και τόσοι δικοί μας πολιτικοί όταν ορκίζονται ότι οσονούπω τελειώνει η αξιολόγηση, ότι σύντομα βγαίνουμε από τα μνημόνια, ότι αρχίζει η ανάπτυξη -- ή ότι ο Μαδούρο προστατεύει το σοσιαλιστικό ιδεώδες. Στο κάτω κάτω αυτά είναι υποσχέσεις, απόψεις ή ερμηνείες. Δεν τρέχει και τίποτα ρε αδερφέ.

Εδώ μιλάμε για τον γάιδαρο. Η διαφωνία μας είναι για το αν πετάει ή όχι. Ο Τραμπ μάς λέει πως πετάει.

Όταν βγαίνει ο πρόεδρος μιας χώρας με τέτοια ισχύ και μας λέει ό,τι του κατέβει, χωρίς να τον εμποδίζει το ότι όλοι οι υπόλοιποι μπορούμε να δούμε το οφθαλμοφανές ψεύδος του, τότε τα πράγματα είναι ήδη πολύ σοβαρά.

Ναι, κάτι τρέχει λοιπόν. Για να μην πω ότι πετάει.

Οπότε καθίσταται επιτακτικό να κάνουμε μια παύση και να κάτσουμε λίγο να σκεφτούμε. Πώς φτάσαμε μέχρι εδώ; Τι κάνουμε; Τι μπορούμε να κάνουμε; Πώς μπορούμε να αμυνθούμε;

Αγαπητοί μου, όσοι από εσάς έχετε παρακολουθήσει τους συλλογισμούς που έχω κατά καιρούς εκθέσει στις επιστολές μου, θα θυμάστε πως ένα από τα θέματα στο οποίο τείνω να επανέρχομαι είναι το θέμα της αλήθειας.

Τη θεωρία του Τάρσκι περί αλήθειας την έχουμε πλέον εμπεδώσει. Έχουμε εξετάσει το τι είναι αληθής πρόταση και τι όχι, έχουμε επισημάνει τα εννοιολογικά προβλήματα της διαφοροποίησης γλώσσας / μεταγλώσσας, έχουμε συζητήσει για την απροσδιοριστία αυτονόητων, τάχα, εννοιών όπως, π.χ., η έννοια "γεγονός", και πάει λέγοντας. Έχουμε περάσει σε επόμενη πίστα.

Όλα εκείνα που λέγαμε είχαν ως στόχο να καταδείξουν πόσο προβληματικά είναι τα διανοητικά εργαλεία που χρησιμοποιούμε και πόσο σημαντικό είναι να γνωρίζουμε τα όριά τους.

Όμως υπήρχε, και συνεχίζει να υπάρχει, ένας μεγάλος κίνδυνος. Αν είχα δίκιο σε αυτά που σας έγραφα, αν πράγματι δεν υπάρχουν "γεγονότα", αν τα πάντα είναι θέμα ορισμού και οπτικής γωνίας, αν είναι προβληματικό το ότι η έννοια της αλήθειας δε νοείται παρά μόνο σε αναφορά προς κάποιο μετα-επίπεδο (και αυτό με τη σειρά του προς κάποιο άλλο μετα-μετα-επίπεδο κ.ο.κ.), αν, αν, αν -- τότε πώς αποφεύγουμε το σχετικισμό του "everything goes";

Διότι αγαπητοί μου, το να λέει κανείς πως έχει στη διάθεσή του "alternative facts", αυτό σημαίνει πως "πετάει ο γάιδαρος, πετάει".

Σημαίνει πως απέναντι στον Τραμπ και τους φίλους του είμαστε απολύτως άοπλοι και ανυπεράσπιστοι.

Και καλά η κυρία τάδε του επιτελείου του. Ο Τραμπ, όμως, έχει το δάχτυλό του στο κουμπί.



Τι κάνουμε λοιπόν;

Κατ' αρχάς διαμαρτυρόμαστε. Με κάθε δυνατό τρόπο. Θα διαβάσατε ίσως για τις πορείες March for Science που διοργανώθηκαν το περασμένο Σάββατο (όχι χτες) σε διάφορες αμερικανικές πόλεις. Επρόκειτο για μια διαμαρτυρία. Αρκετά ηχηρή μάλιστα.

Ηχηρή, αλλά, λυπάμαι που θα σας στεναχωρήσω, περιορισμένης αποδοτικότητας.

Το τσουνάμι του ανορθολογισμού του Τραμπ και των "εναλλακτικών δεδομένων" του δεν αντιμετωπίζεται με πορείες και κλαψουρίσματα για το πόσο χρήσιμη είναι η επιστήμη.

Το κακό είναι πως οι θεράποντες του ορθού λόγου είναι τόσο πεπεισμένοι πως μιλάνε για την "αλήθεια", τόσο πεπεισμένοι για την ορθότητα της προσέγγισής τους, ώστε τείνουν να παραβλέπουν πως η ορθότητα αυτή μπορεί να οριστεί (και να εννοηθεί) μόνο σε σαφώς προσδιορισμένα εννοιολογικά πλαίσια και όχι έτσι γενικώς.

Καταλήγουν να μιλούν για τα πάντα με αυθεντία και ναρκισσιστική αυταρέσκεια. Στα μάτια των θιασωτών της επιστήμης και του ορθού λόγου, αν δεν είσαι μαζί τους, είσαι εναντίον τους.

Βλέπουν τον Τραμπ και τους οπαδούς του και τους περιγελούν με περιφρόνηση.

Όμως σε κανέναν δεν αρέσει να τον κοιτάνε αφ' υψηλού ή να τον περιγελούν με περιφρόνηση. Εντάξει, ο Τραμπ δεν μασάει. Αλλά οι οπαδοί του το φέρουν βαρέως. Άλλο πράγμα το να μην καταλαβαίνεις κάτι, και άλλο η όλη συζήτηση να σε κάνει να νοιώθεις αμελητέος, αποξενωμένος και ανύπαρκτος.

Λόγω της αυταρέσκειας των εκπροσώπων της, το δέος και ο σεβασμός που θα ήταν εύλογο να μας προκαλεί η επιστήμη μετατρέπονται σε απαξίωση.

Αυτό που βλέπουμε σήμερα είναι η σύγχυση μεταξύ απαξίωσης και αντισυστημισμού.

Απέναντι στην αυταρέσκεια των επιστημονάδων που μετρούν τη χωρητικότητα του νου σε petabyte, σταμπάρουν τον καθένα μας ως φορέα της μίας ή της άλλης διαταραχής, και μπουκώνουν μικρά παιδιά με ψυχοφάρμακα γιατί δεν μπορούν να τα κάνουν να κάτσουν ήσυχα, πολλοί καταλήγουν στο συμπέρασμα πως η μόνη σου άμυνα είναι ο Τραμπ και τα εναλλακτικά του γεγονότα.

Πώς το έλεγε ο παρ' ημίν Πρωθυπουργός (ΤΜ) όταν του λέγανε κάτι οπαδοί, ξέρω 'γω, πως δεν διαβάζουν εφημερίδες; "Την καλύτερη δουλειά κάνετε." Αυτό.

Και όχι μόνο ο Τραμπ. Πάρτε το Μπρέξιτ. Όλοι οι ειδικοί ξεσπάθωσαν εναντίον του. Επιστήμονες, οικονομολόγοι, οραματιστές, μελλοντολόγοι -- όλοι εξήγησαν, όσο πιο καθαρά μπορούσαν, πόσο καταστροφικό θα ήταν.

Άδικα ιδρώνανε. Τους μόνους που κατάφεραν να πείσουν ήταν τους ήδη πεπεισμένους. Οι υπόλοιποι ψήφισαν Φάρατζ και Μπρέξιτ.

Τον Φάρατζ! Εναν τύπο γκάου που αν τον πετύχαινες σε καμιά καφετέρια πριν καμιά τριανταριά χρόνια θα καθόσουν στην άλλη άκρη για να μην σου βγει το κακό όνομα στα μωρά.

Και στην Αμερική ψήφισαν τον Τραμπ! Με την καροτί του φράντζα και τον προβληματικό μορφασμό. ΟΚ, και τα λεφτά και τη χάι κόρη.

Και στη Γαλλία την Λεπέν! (No further comment.)

Όχι. Δεν γίνεται να αμυνθείς στον Τραμπ και τους φίλους του με "πορείες για την επιστήμη" και άλλα τέτοια ρομαντικά.

Η ανορθολογικότητα του Τραμπ, η αδιαφορία του για το τι είναι ορθός συλλογισμός και σωστή επιχειρηματολόγηση, καθίσταται το βασικότερό του όπλο. Όσο πιο εξόφθαλμο το ψεύδος, τόσο πιο γοητευτικός ο λόγος του. Όσο πιο εξωφρενικός ο ισχυρισμός του, τόσο πιο ελκυστικές οι υποσχέσεις του.

Δεν ξέρω πώς μπορείς να αμυνθείς. Δεν ξέρω καν αν μπορείς.

Λοιπόν, έρχεται το καράβι. Σας αφήνω.

Άστα λουέγο κομπανιέρος. Τα λέμος.

Σας ασπάζομαι,
Θείος Ακάκιος

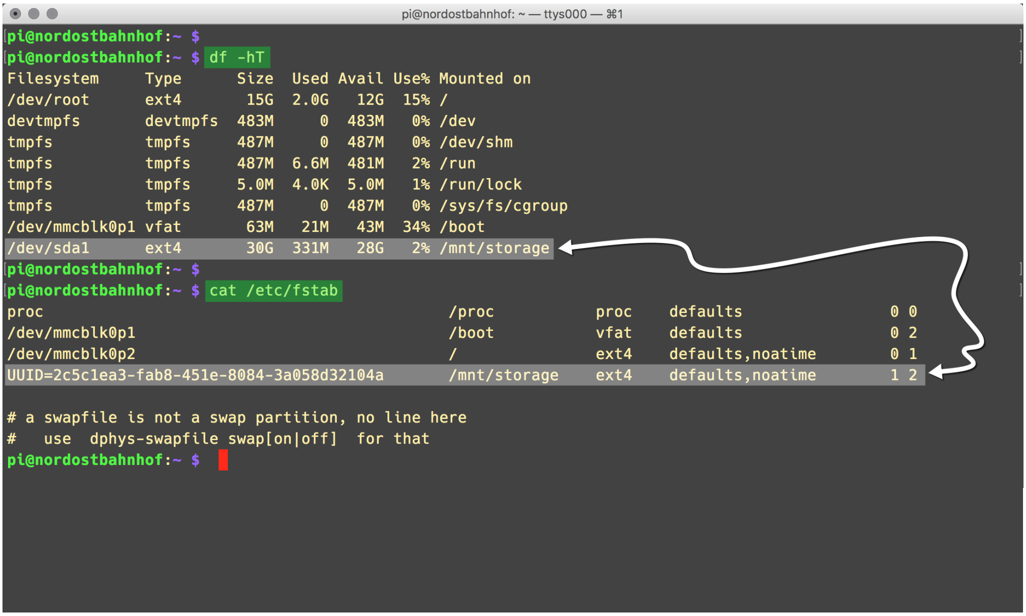
Skill: Intermediate
Tags: Nextcloud, MariaDB, HSTS, PHP, Raspberry Pi

Nextcloud στο Raspberry Pi, από την καλή

Με λίγη προετοιμασία το Raspberry Pi μεταμορφώνεται σε άξιο αντικαταστάτη του Dropbox. Στο παρόν άρθρο δείχνουμε πώς εγκαθιστούμε και ρυθμίζουμε το Nextcloud, τον διάδοχο του ownCloud, στο ταπεινό αλλά ικανότατο Raspberry. Θα δούμε επίσης πώς ενισχύουμε την ασφάλεια αλλά και πώς βελτιώνουμε τις επιδόσεις της πλατφόρμας.

Το Nextcloud (https://nextcloud.com) είναι σχετικά απαιτητικό σε πόρους συστήματος και μεταξύ των συσκευών Raspberry προτείνεται να το φιλοξενήσουμε στο νεότερο μοντέλο, δηλαδή στο Raspberry Pi 3 model B. Υποθέτουμε ότι η συσκευή θα τρέχει το Raspbian. Για την εγκατάσταση και τη ρύθμιση του συγκεκριμένου λειτουργικού μπορείτε να διαβάσετε το άρθρο στο https://deltahacker.gr/?p=16992. Στο Raspbian εξάλλου θα είναι εγκατεστημένος ο Apache, τον οποίο χρειαζόμαστε για την πρόσβαση στο web panel του Nextcloud. Το site που σερβίρει ο Apache καλύπτεται από δωρεάν κι έγκυρο πιστοποιητικό, το οποίο έχει εκδοθεί από το εγχείρημα Let's Encrypt. Προκειμένου ν' αποκτήσετε κι εσείς πιστοποιητικό για το domain ή το subdomain σας, δείτε το αναλυτικό άρθρο στο https://deltahacker.gr/?p=17024. Στο πλαίσιο της παρουσίασής μας χρησιμοποιούμε το subdomain ονόματι nue.colder.xyz.

Σημείωση: Στο Raspberry Pi προτείνεται να έχουμε συνδεδεμένο κάποιο εξωτερικό μέσο αποθήκευσης. Η κάρτα SD, στην οποία κατοικοεδρεύει το Raspbian, υπό καμία έννοια δεν είναι κατάλληλη για χρήση από file server. Σε κάθε περίπτωση, με ένα USB thumb drive ή ακόμα καλύτερα με έναν δίσκο USB (όχι κατ' ανάγκη SSD), έχουμε πολύ περισσότερο αποθηκευτικό χώρο και σαφώς ανεβασμένες επιδόσεις.



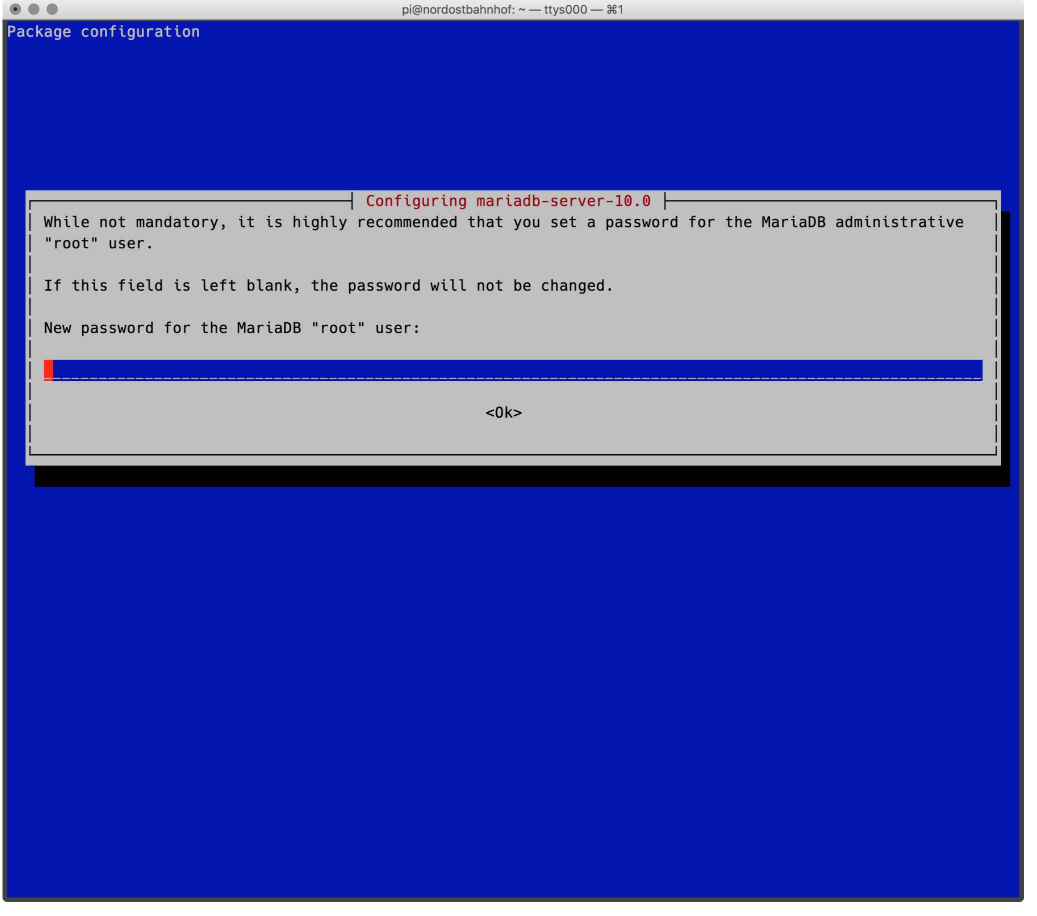
Για τις ανάγκες της παρουσίασής μας, στο Raspberry Pi έχουμε συνδέσει ένα USB thumb drive χωρητικότητας 32GB. Η αντίστοιχη κατάτμηση είναι προσαρτημένη κάτω από το /mnt/storage κι εκεί, λίγο αργότερα, θα μεταφέρουμε το data directory του Nextcloud. Στο δε /etc/fstab έχουμε προσθέσει μία κατάλληλη γραμμή ώστε η κατάτμηση του thumb drive, την οποία υποδεικνύουμε με βάση το UUID της, να προσαρτάται αυτόματα κατά την εκκίνηση του λειτουργικού.

Εγκατάσταση PHP5 και MariaDB

Το Nextcloud χρειάζεται τη σκριπτογλώσσα PHP καθώς και μία βάση δεδομένων. Σε διάφορες εγκαταστάσεις θα δείτε ότι το ρόλο συστήματος διαχείρισης βάσεων τον έχει η SQLite. Δεν αποτελεί την καλύτερη επιλογή όσον αφορά στις επιδόσεις, οπότε εμείς θα στραφούμε στη MariaDB. Προχωράμε αμέσως στην εγκατάσταση όλων των σχετικών πακέτων:

```
pi@nordostbahnhof:~ $ sudo apt-get update
pi@nordostbahnhof:~ $ sudo apt-get -y install mariadb-common mariadb-client
mariadb-server php5 php5-common php5-cli php5-json php5-readline php5-gd php5-
curl php5-mysql
```

Η MariaDB αναπτύσσεται από την κοινότητα Ανοικτού/Ελεύθερου Λογισμικού και είναι fork της γνωστής MySQL, η οποία από το 2010 ανήκει στην Oracle. Θα παρατηρήσετε ότι παρά την επιλογή μας, ορισμένα πακέτα περιλαμβάνουν το όνομα της MySQL (π.χ., php5-mysql). Το ίδιο ισχύει και με κάποια εργαλεία κι εντολές που θα χρησιμοποιήσουμε σε πολύ λίγο (π.χ., mysql, mysql_secure_installation κ.ά.). Το γεγονός αυτό δεν πρέπει να μας προκαλεί εντύπωση, αφού η MariaDB έχει σχεδιαστεί ως drop-in replacement της MySQL.



Κατά την εγκατάσταση της MariaDB μάς ζητείται να ορίσουμε ένα συνθηματικό για τον χρήστη root. Προσοχή: Μιλάμε για τον root της MariaDB – η συνωνυμία με τον root του λειτουργικού συστήματος είναι εντελώς συμπτωματική.

Αμέσως μετά την εγκατάσταση της MariaDB είναι καλό να φροντίσουμε για ορισμένες ρυθμίσεις που αφορούν στην ασφάλεια. Καταφεύγουμε στο εργαλείο mysql_secure_installation, το οποίο τρέχουμε με δικαιώματα διαχειριστή συστήματος:

```
pi@nordostbahnhof:~ $ sudo mysql_secure_installation
```

Θα μας απευθυνθούν μια σειρά από ερωτήσεις. Εκτός ίσως από την πρώτη, η οποία αφορά στον καθορισμό password για τον root της MariaDB, σε όλες τις υπόλοιπες ερωτήσεις προτείνεται ν' αφήνουμε την προεπιλεγμένη απάντηση.

```
pi@nordostbahnhof: ~ — ttys000 — ⌘1
pi@nordostbahnhof:~ $ sudo mysql_secure_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user.  If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

You already have a root password set, so you can safely answer 'n'.

Change the root password? [Y/n] n
 ... skipping.

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
```

Κατά την εγκατάσταση της MariaDB είχαμε ορίσει password για τον root, οπότε δεν χρειάζεται να το κάνουμε τώρα. Συμφωνούμε, όμως, με τη διαγραφή του λογαριασμού του ανώνυμου χρήστη.

```
pi@nordostbahnhof: ~ — ttys000 — ⌘1

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
 ... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
 - Dropping test database...
 ... Success!
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
 ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
pi@nordostbahnhof:~ $
```

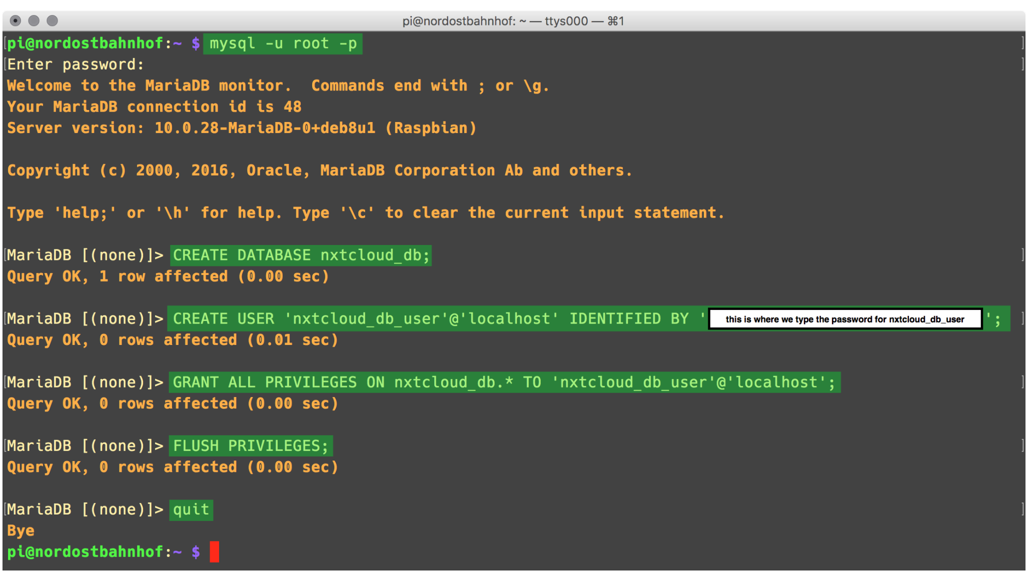
Για λόγους ασφαλείας απαγορεύουμε τις απομακρυσμένες συνδέσεις στο λογαριασμό root της MariaDB, ενώ διαγράφουμε και τη δοκιμαστική βάση δεδομένων με όνομα 'test'.

Δημιουργία βάσης και χρήστη στη MariaDB

Θα φτιάξουμε τώρα μία νέα βάση δεδομένων για τη MariaDB, την οποία θα χρησιμοποιεί το Nextcloud. Η βάση από μόνη της δεν αρκεί, χρειάζεται κι ένας λογαριασμός χρήστη –της MariaDB– με πλήρη δικαιώματα επί της βάσεως. Αυτόν το λογαριασμό, ουσιαστικά, θα χρησιμοποιεί το Nextcloud, ώστε να έχει πρόσβαση στη βάση. Παραθέτουμε τις εντολές για τη δημιουργία της νέας βάσης, του νέου λογαριασμού, καθώς και της απόδοσης των σχετικών δικαιωμάτων πρόσβασης:

```
pi@nordostbahnhof:~ $ mysql -u root -p
MariaDB [(none)]> CREATE DATABASE nxtcloud_db;
MariaDB [(none)]> CREATE USER 'nxtcloud_db_user'@'localhost' IDENTIFIED BY
                  'nxtcloud_db_user_passwd';
MariaDB [(none)]> GRANT ALL PRIVILEGES ON nxtcloud_db.* TO 'nxtcloud_db_
                  user'@'localhost';
MariaDB [(none)]> FLUSH PRIVILEGES;
MariaDB [(none)]> QUIT
```

Το όνομα της νέας βάσης είναι nxtcloud_db, το όνομα του νέου χρήστη είναι nxtcloud_db_user, το δε password του είναι το nxtcloud_db_user_passwd. Καταλαβαίνετε τώρα ότι στο σημείο αυτό είμαστε υποχρεωμένοι να υπογραμμίσουμε ότι για τον *δικό σας* χρήστη, όπως κι αν τον ονομάσετε, θα πρέπει να ορίσετε διαφορετικό password. Προσέξτε: Ούτε για μια στιγμή δεν πέρασε από το μυαλό μας η ιδέα πως δεν θα ορίζατε διαφορετικό password για τον χρήστη σας. Απλά, αισθανόμαστε υποχρεωμένοι να κάνουμε τη σχετική παρατήρηση. Και τώρα που την κάναμε, η ιδέα που προηγουμένως δεν επρόκειτο να περάσει καν από το μυαλό μας, ε, πέρασε ήδη.



Δημιουργία νέας βάσης δεδομένων και χρήστη της MariaDB, για τις ανάγκες του Nextcloud.

Λήψη κι εγκατάσταση του Nextcloud

Πηγαίνουμε στο

https://download.nextcloud.com/server/releases

και ψάχνουμε για την πλέον πρόσφατη έκδοση του Nextcloud. Τη στιγμή που γράφονται αυτές οι γραμμές, η νεότερη έκδοση είναι η 11.0.0. Την κατεβάζουμε στο RasPi με τη βοήθεια του εργαλείου wget:

```
pi@nordostbahnhof:~ $ mkdir incoming && cd incoming
pi@nordostbahnhof:~/incoming $ wget https://download.nextcloud.com/server/
releases/nextcloud-11.0.0.zip
```

Αποσυμπιέζουμε το αρχείο ZIP με το εργαλείο unzip:

```
pi@nordostbahnhof:~/incoming $ unzip nextcloud-11.0.0.zip
```

Θα δημιουργηθεί ο κατάλογος nextcloud...

```
pi@nordostbahnhof:~/incoming $ ls -lh
total 48M
drwxr-xr-x 14 pi pi 4.0K Dec 13 13:25 nextcloud
-rw-r--r--  1 pi pi  48M Dec 13 14:34 nextcloud-11.0.0.zip
```

...τον οποίο πρέπει να μεταφέρουμε στο /var/www/html, δηλαδή στο προκαθορισμένο DocumentRoot του Apache στο Raspbian:

```
pi@nordostbahnhof:~/incoming $ sudo mv nextcloud /var/www/html
```

Κατ' αυτόν τον τρόπο, στο web panel του Nextcloud θα φτάνουμε πληκτρολογώντας τη διεύθυνση

https://nue.colder.xyz/nextcloud

(στη θέση του nue.colder.xyz θα βάζετε το δικό σας (sub)domain). Αν τώρα θέλετε να *μην* πληκτρολογείτε το '/nextcloud' στο URL, τότε αντί να μεταφέρετε τον κατάλογο nextcloud κάτω από το /var/www/html θα μεταφέρετε το *περιεχόμενο* του nextcloud κάτω από το /var/www/html.

Φτιάχνουμε τώρα το data directory του Nextcloud, δηλαδή τον κατάλογο εντός του οποίου αποθηκεύονται όλα τα αρχεία που ανεβάζουμε στο RasPi και διαχειρίζεται η πλατφόρμα. Η προκαθορισμένη θέση για το data directory είναι η /var/www/html/nextcloud, γεγονός που για την περίπτωσή μας σημαίνει ότι το data θα

βρίσκεται πάνω στην κάρτα SD. Δεν πρόκειται για την καλύτερη δυνατή θέση, τόσο για λόγους επιδόσεων όσο και ασφαλείας. Προς το παρόν όμως ας δημιουργήσουμε το data στην προκαθορισμένη θέση και λίγο αργότερα το μεταφέρουμε αλλού:

```
pi@nordostbahnhof:~/incoming $ sudo mkdir /var/www/html/nextcloud/data
```

Ο κατάλογος πρέπει να ανήκει στο χρήστη και στην ομάδα www-data:

```
pi@nordostbahnhof:~/incoming $ sudo chown www-data:www-data /var/www/html/
nextcloud/data
```

Φροντίζουμε και για τα δικαιώματα πρόσβασης:

```
pi@nordostbahnhof:~/incoming $ sudo chmod 750 /var/www/html/nextcloud/data
```

Πριν προχωρήσουμε στη ρύθμιση του Nextcloud, αλλάζουμε το ιδιοκτησιακό καθεστώς των καταλόγων config και apps, κάτω από τον κατάλογο /var/www/html/nextcloud:

```
pi@nordostbahnhof:~/incoming $ cd /var/www/html/nextcloud
pi@nordostbahnhof:/var/www/html/nextcloud $ sudo chown www-data:www-data config
apps
```

Πρώτη ρύθμιση Nextcloud

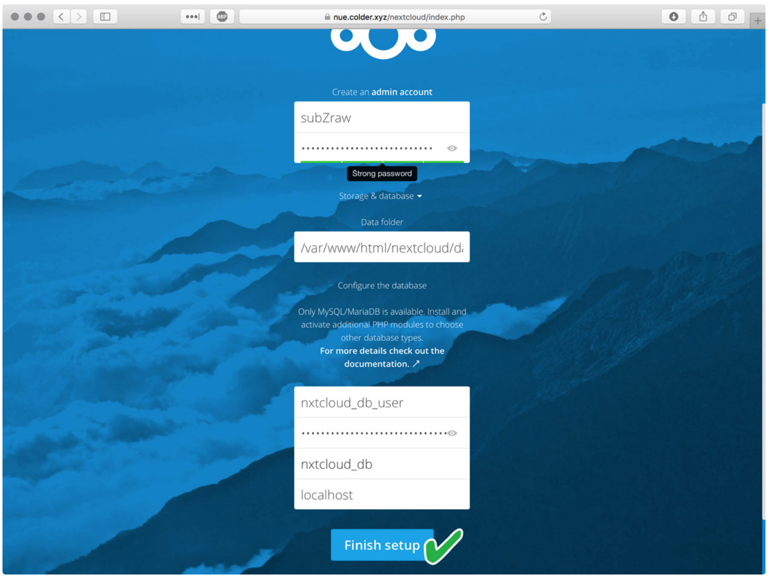
Στη μπάρα διευθύνσεων του web browser της προτίμησής μας, πληκτρολογούμε τη διεύθυνση

https://nue.colder.xyz/nextcloud

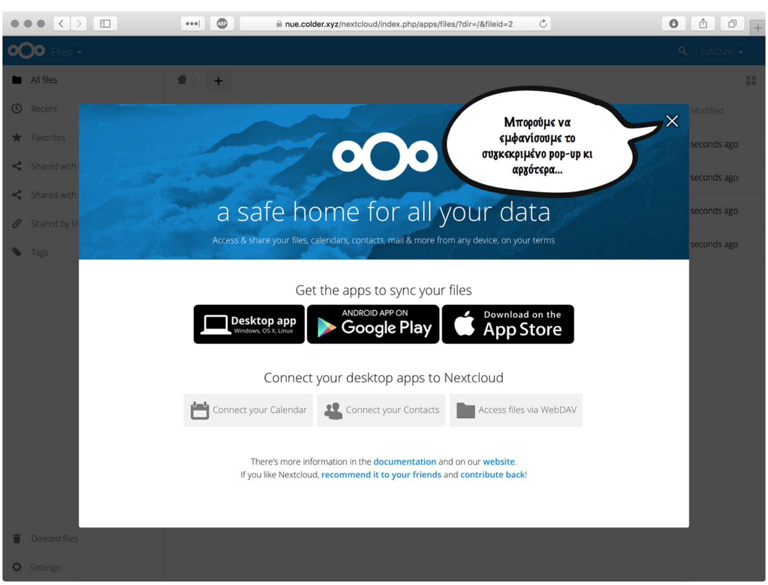
Στη σελίδα που εμφανίζεται συμπληρώνουμε τα ακόλουθα στοιχεία:

- username και password για το νέο χρήστη του Nextcloud (πρόκειται για λογαριασμό με δικαιώματα διαχειριστή και η δημιουργία του είναι υποχρεωτική)
- την πλήρη διαδρομή του καταλόγου data (π.χ., /var/www/html/nextcloud/data)
- το username του χρήστη της MariaDB, ο οποίος έχει πλήρη δικαιώματα στη βάση που φτιάξαμε για το Nextcloud
- το password του προαναφερθέντος χρήστη
- το όνομα της βάσης της MariaDB, που δημιουργήσαμε για το Nextcloud

Επικυρώνουμε με ένα κλικ στο κουμπί Finish setup, στο κάτω μέρος της σελίδας. Αν όλα έχουν πάει καλά, αντικρίζουμε τώρα τη σελίδα καλωσορίσματος του Nextcloud. Υπάρχουν κάποιες προτάσεις για clients διαφόρων λειτουργικών συστημάτων, ώστε να συγχρονίζουμε εύκολα αρχεία και καταλόγους με το Nextcloud. Προς το παρόν κλείνουμε το pop-up με τις προτάσεις. Ούτως ή άλλως, ανά πάσα στιγμή μπορούμε να το εμφανίσουμε και πάλι.



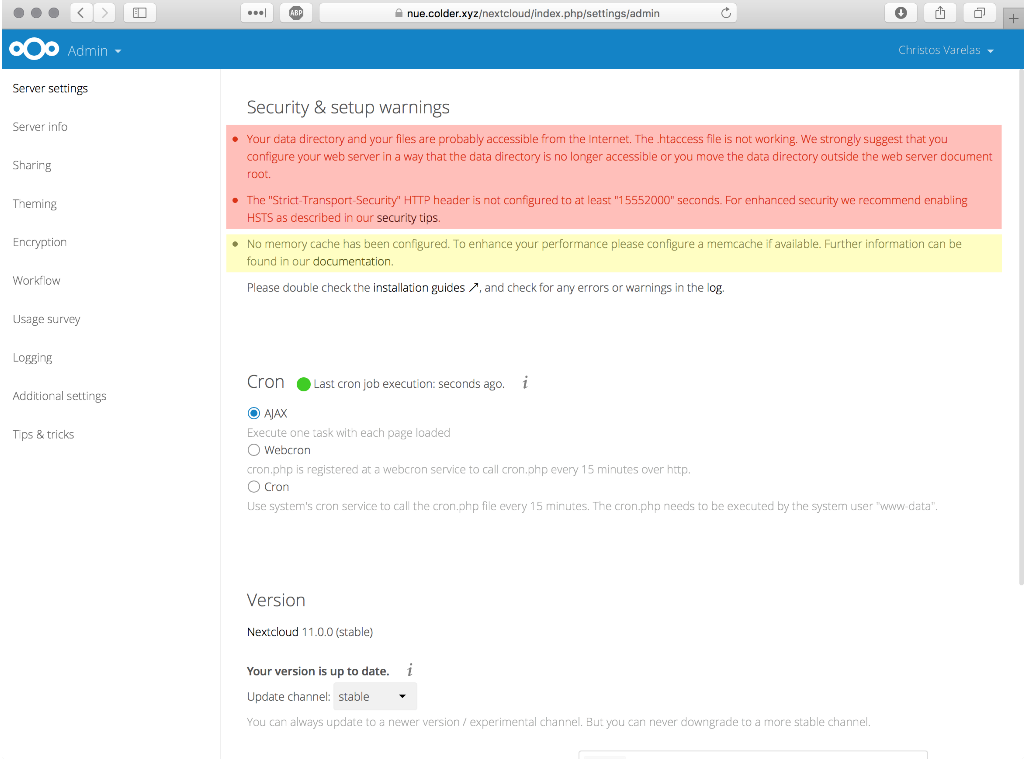
Η αρχική ρύθμιση του Nextcloud περιλαμβάνει τη δημιουργία ενός λογαριασμού χρήστη για την πλατφόρμα με δικαιώματα διαχειριστή, την υπόδειξη της θέσης του data directory, τον καθορισμό της βάσης δεδομένων που φτιάξαμε για το Nextcloud – βεβαίως και τον καθορισμό του χρήστη με δικαιώματα διαχειριστή επί της βάσης.



Η σελίδα καλωσορίσματος του Nextcloud, μετά την επιτυχή εγκατάσταση και τις πρώτες βασικές ρυθμίσεις. Πριν αρχίσουμε να χρησιμοποιούμε την πλατφόρμα, μένουν μερικές ακόμα διευθετήσεις που οφείλουμε να κάνουμε.

Ενίσχυση της ασφάλειας

Έχοντας συνδεθεί στο λογαριασμό του χρήστη μας στο Nextcloud από το web panel της πλατφόρμας, κάνουμε κλικ στο username πάνω δεξιά κι από το μενού που εμφανίζεται επιλέγουμε το Admin. Στο πάνω μέρος της νέας σελίδας που φορτώνει υπάρχουν τρεις προειδοποιήσεις – ή τουλάχιστον τόσες ήταν στη δική μας περίπτωση. Οι δύο πρώτες αφορούν στην ασφάλεια και η τρίτη στις επιδόσεις του Nextcloud. Στη συνέχεια θα φροντίσουμε ώστε όλες τους να εξαφανιστούν.



Προειδοποιήσεις περί ασφάλειας κι επιδόσεων της εγκατάστασης του Nextcloud που μόλις πραγματοποιήσαμε. Δεν πρέπει να τις αγνοήσουμε – ειδικά εκείνες που αφορούν στην ασφάλεια.

Νομίζουμε ότι η πρώτη προειδοποίηση είναι σαφής: το data directory του Nextcloud δεν πρέπει να βρίσκεται κάτω από το DocumentRoot του Apache. Προς το παρόν είναι μέσα στο /var/www/html/nextcloud, άρα εκεί που δεν πρέπει να βρίσκεται :) Από τη μεριά μας φτιάξαμε τον κατάλογο nextcloud κάτω από το /mnt/storage και μεταφέραμε το data εκεί. Στο /mnt/storage είναι προσαρτημένο ένα USB thumb drive, οπότε μεταφέροντας τον κατάλογο data κερδίσαμε τόσο σε ασφάλεια όσο και σε επιδόσεις:

```
pi@nordostbahnhof:~ $ sudo mkdir /mnt/storage/nextcloud
pi@nordostbahnhof:~ $ sudo mv /var/www/html/nextcloud/data /mnt/storage/
nextcloud/
```

Μετά τη μεταφορά του καταλόγου data πρέπει, φυσικά, να ενημερώσουμε σχετικά και το Nextcloud. Αρκεί να τροποποιήσουμε την τιμή της παραμέτρου datadirectory, στο αρχείο ρυθμίσεων config.php κάτω από το /var/www/html/nextcloud/config. Πριν κάνουμε την αλλαγή μας, είναι καλή ιδέα να κρατήσουμε ένα αντίγραφο του config.php. Δείτε:

```
pi@nordostbahnhof:~ $ cd /var/www/html/nextcloud/config
pi@nordostbahnhof:/var/www/html/nextcloud/config $ sudo cp -p config.php config.
php.ORIG
pi@nordostbahnhof:/var/www/html/nextcloud/config $ sudo vi config.php
```

Στο παράδειγμά μας ανοίγουμε το config.php με το vi, εννοείται όμως ότι μπορείτε να το ανοίξετε με έναν οποιονδήποτε άλλο text editor (π.χ., με το nano). Όπως και να 'χει, εντοπίζουμε τη γραμμή

```
'datadirectory' => '/var/www/html/nextcloud/data',
```

και την αλλάζουμε σε

```
'datadirectory' => '/mnt/storage/nextcloud/data',
```

Προσοχή χρειάζεται με το κόμμα, το οποίο δεν πρέπει να διαγράψουμε! Αποθηκεύουμε τις αλλαγές στο config.php κι εγκαταλείπουμε τον editor. Κάνοντας reload στη σελίδα του Nextcloud με τις προειδοποιήσεις, διαπιστώνουμε ότι εκείνη περί της θέσης του καταλόγου data δεν υπάρχει πια. Καλό αυτό.

Στρέφουμε τώρα την προσοχή μας στην άλλη προειδοποίηση ασφαλείας, σχετικά με το HSTS. Θέτοντας την κατάλληλη τιμή στο HTTP Strict Transport Security header, διασφαλίζουμε ότι στους clients του Nextcloud δεν θα επιτρέπονται απλές συνδέσεις HTTP. Προσέξτε: Ο Apache μας είναι έτσι ρυθμισμένος ώστε να ανακατευθύνει τις συνδέσεις HTTP σε συνδέσεις HTTPS. Χωρίς όμως το Strict Transport Security header, η υλοποίηση επιθέσεων Man-in-The-Middle είναι εφικτή. Για το HSTS, με δικαιώματα διαχειριστή ανοίγουμε το αρχείο /etc/apache2/sites-available/000-default-le-ssl.conf...

```
pi@nordostbahnhof:~ $ sudo vi /etc/apache2/sites-available/000-default-le-ssl.
conf
```

και στο τέλος της ενότητας <VirtualHost *:443> ... </VirtualHost> προσθέτουμε τις ακόλουθες τρεις γραμμές:

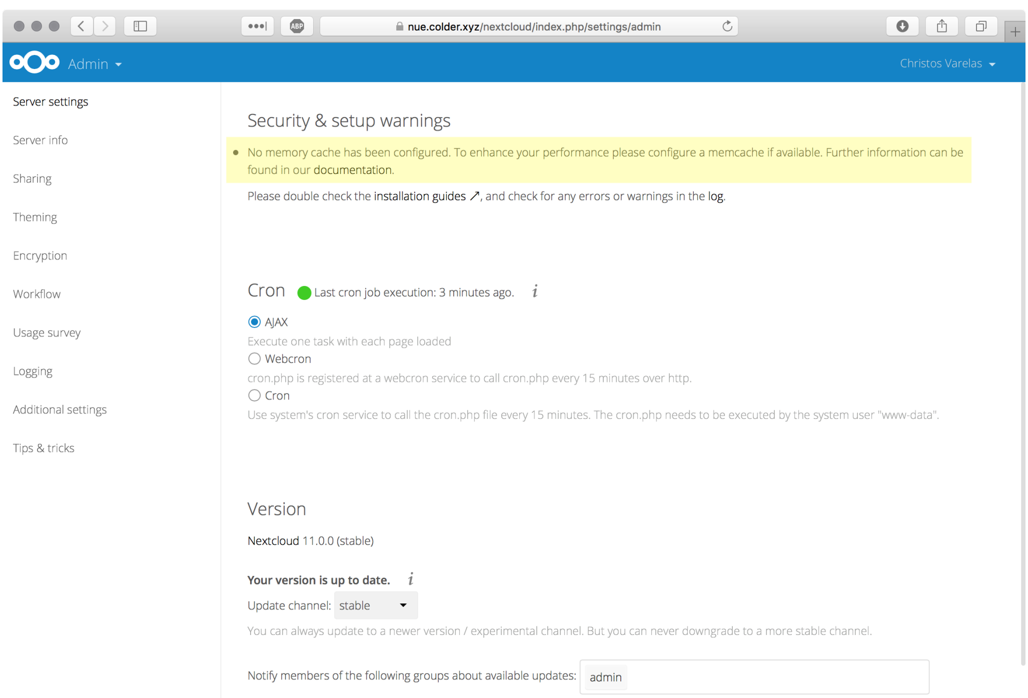
```
<IfModule mod_headers.c>
      Header always set Strict-Transport-Security "max-age=15552000;
includeSubDomains; preload"
</IfModule>
```

Αποθηκεύουμε τις αλλαγές στο 000-default-le-ssl.conf, εγκαταλείπουμε τον editor, φορτώνουμε το module του Apache ονόματι headers...

```
pi@nordostbahnhof:~ $ sudo a2enmod headers
```

...κι επανεκκινούμε τον Apache:

```
pi@nordostbahnhof:~ $ sudo systemctl restart apache2.service
```



Οι δύο ειδοποιήσεις περί θεμάτων ασφαλείας έχουν εξαφανιστεί κι αυτή τη στιγμή έχουμε μόνο μία, η οποία αφορά στις επιδόσεις της πλατφόρμας.

Με refresh στη σελίδα Admin του Nextcloud διαπιστώνουμε ότι η προειδοποίηση για το HSTS έχει εξαφανιστεί. Ως έξτρα μπόνους, κάνοντας στο https://www.ssllabs.com το SSL test για το site του Nextcloud (για εμάς είναι το https://nue.colder.xyz), η τελική βαθμολογία που παίρνουμε δεν είναι απλά 'A' αλλά 'A+'!

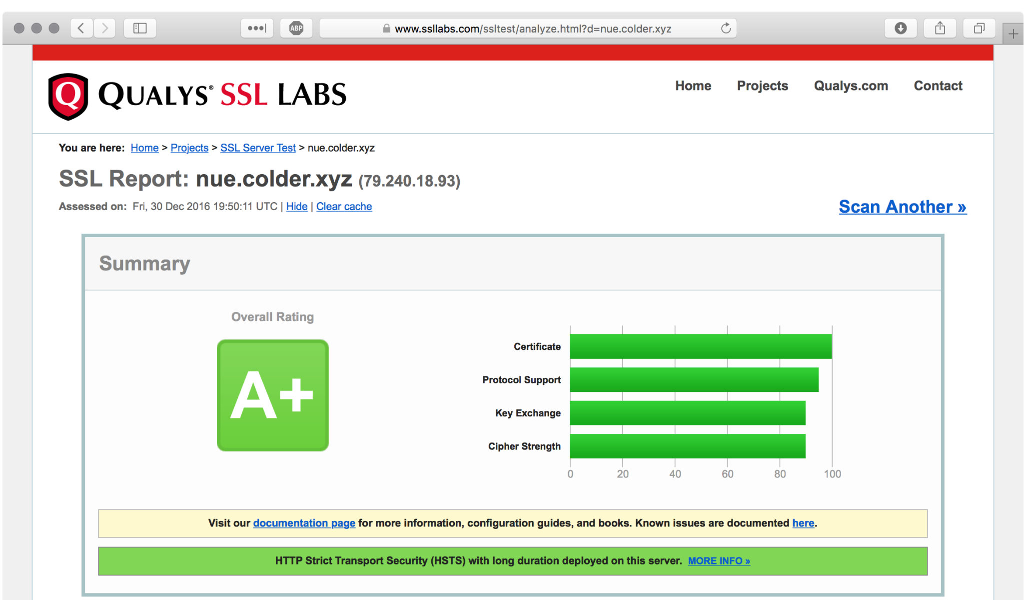
Βελτίωση επιδόσεων και συμπεριφορά της PHP

Προς το παρόν δεν υπάρχει κάποιος μηχανισμός memory caching ενεργοποιημένος για το Nextcloud — κι αυτό έχει αρνητική επίδραση στις επιδόσεις της πλατφόρμας. Σε λίγο θα ενεργοποιήσουμε το σύστημα memory caching ονόματι APCu (κατάλληλο για την PHP5 που χρησιμοποιούμε), έτσι τα αντικείμενα που ζητούνται συχνά από τους clients θα διατηρούνται στη μνήμη του RasPi και συνεπώς η πρόσβαση σ' αυτά θα γίνεται πολύ γρηγορότερα. Ξεκινάμε εγκαθιστώντας το πακέτο php5-apcu...

```
pi@nordostbahnhof:~ $ sudo apt-get install php5-apcu
```

κι αμέσως μετά επανεκκινούμε τον Apache:

```
pi@nordostbahnhof:~ $ sudo systemctl restart apache2.service
```

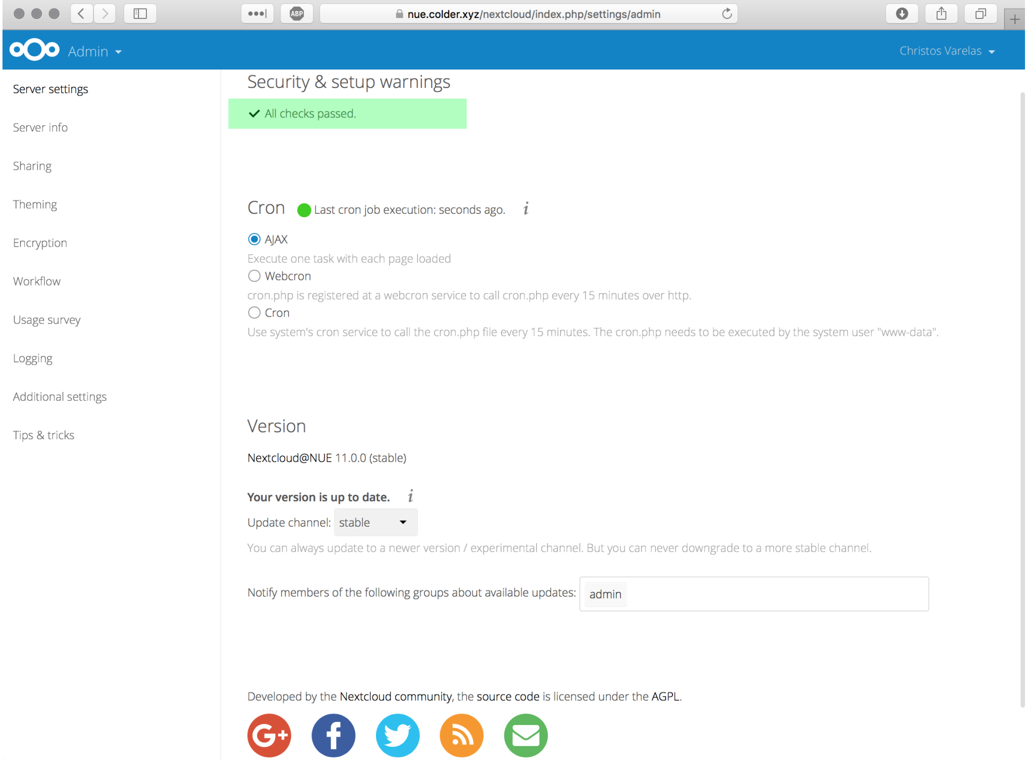


Χάρη στο HTTP Strict Transport Security header που θέσαμε για το site του Nextcloud, τους ελέγχους του SSL Labs τους περνάμε με βαθμολογία 'A+'. Θυμόσαστε τη βαθμολογία που είχαμε πάρει μετά την εφαρμογή των οδηγιών του άρθρου 'O Apache στο Raspberry Pi, με έγκυρο πιστοποιητικό'; Ήταν 'A' σκέτο :/

Με τον text editor της επιλογής μας και δικαιώματα διαχειριστή (sudo), ανοίγουμε το αρχείο /var/www/html/nextcloud/config/config.php. Σε μια νέα γραμμή πάνω από την τελευταία παρένθεση, εισάγουμε την ακόλουθη οδηγία:

```
'memcache.local' => '\OC\Memcache\APCu',
```

(προσοχή, το κόμμα χρειάζεται). Αποθηκεύουμε την αλλαγή στο config.php κι εγκαταλείπουμε τον editor. Επιστρέφοντας στον web browser, φρεσκάρουμε τη σελίδα Admin του Nextcloud. Αν όλα έχουν πάει καλά τότε η προειδοποίηση περί memory caching θα έχει εξαφανιστεί. Λογικά, δεν θα υπάρχει καμία προειδοποίηση.



Μετά τις παρεμβάσεις μας, στη σελίδα Admin του Nextcloud δεν υπάρχει καμία προειδοποίηση. Όχι μόνο αυτό, αλλά παίρνουμε κι αυτό το ευχάριστο μήνυμα για όλους εκείνους τους ελέγχους που έγιναν επιτυχώς κι αυτή τη στιγμή η ζωή δύσκολα θα μπορούσε να 'ναι πιο ωραία.

Προτάσεις για τη συνέχεια

Ο καλύτερος τρόπος για να στέλνουμε αρχεία στο Nextcloud καθώς και για να τα συγχρονίζουμε (επιλεκτικά) μεταξύ των συσκευών μας, είναι με τη βοήθεια του κατάλληλου client για το εκάστοτε λειτουργικό σύστημα. Αν κάνουμε κλικ στο όνομα του χρήστη μας (πάνω δεξιά), από το μενού που εμφανίζεται διαλέξουμε το

Personal, στην οριζόντια μπάρα αριστερά πατήσουμε στο Sync clients και κάνουμε κι ένα τελευταίο κλικ στο κουμπί Show First Run Wizard again (δεξιά), εμφανίζεται τότε ένα pop-up για επιλογή client: είναι αυτό που είχαμε δει αμέσως μετά την επιτυχή ρύθμιση του Nextcloud.

Στις δικές σας συσκευές προτείνουμε να κατεβάσετε και να εγκαταστήσετε τον κατάλληλο Nextcloud client. Όσοι χρησιμοποιείτε Dropbox θα διαπιστώσετε ότι σε γενικές γραμμές ακολουθείται η ίδια λογική: υποδεικνύουμε έναν τοπικό κατάλογο, τα περιεχόμενα του οποίου συγχρονίζονται αυτόματα με τον ίδιο κατάλογο στον server. Φυσικά, σε κάθε συσκευή μπορούμε να υποδεικνύουμε υποκαταλόγους οι οποίοι ναι μεν βρίσκονται στον server, αλλά δεν συγχρονίζονται με τον συγκεκριμένο client.

Θα υπάρξουν βέβαια και οι περιπτώσεις όπου θα χρειάζεται ν' ανεβάσουμε στο Nextcloud ένα ή περισσότερα αρχεία, όμως στον υπολογιστή από τον οποίο εργαζόμαστε αφενός δεν θα υπάρχει client, αφετέρου δεν θα θέλουμε ή/και δεν θα μπορούμε να εγκαταστήσουμε έναν. Κανένα πρόβλημα: Ανά πάσα στιγμή μπορούμε ν' ανεβάζουμε αρχεία μέσω του web browser (αφού φυσικά συνδεθούμε στο λογαριασμό μας στο Nextcloud). Ουσιαστικά, το uploading το αναλαμβάνει η PHP. Έτσι όπως είναι το σχετικό αρχείο ρυθμίσεων, υπάρχει ένα όριο στο μέγεθος των αρχείων που ανεβάζουμε κι αυτό το όριο είναι τα 2MB. Πιθανώς να το βρείτε κάπως περιοριστικό, οπότε θα θελήσετε να το αλλάξετε. Προς τούτο, με δικαιώματα διαχειριστή ανοίγουμε το αρχείο /etc/php5/apache2/php.ini, εντοπίζουμε τις ακόλουθες δύο γραμμές

```
post_max_size = 8M
upload_max_filesize = 2M
```

(δεν είναι μαζί) κι αλλάζουμε τις τιμές για τις δύο παραμέτρους. Για παράδειγμα, στο δικό μας php.ini ισχύει:

```
post_max_size = 16M
upload_max_filesize = 16M
```

Αυτή τη στιγμή η εγκατάσταση του Nextcloud στο Raspberry Pi είναι πανέτοιμη! Υπάρχουν αρκετά που θέλουμε να δείξουμε αναφορικά με τη συγκεκριμένη πλατφόρμα, ενώ υπάρχουν και κάποιες γενικές στρατηγικές backup που έχουμε κατά νου και θα θέλαμε να συζητήσουμε. Το επόμενο διάστημα θα επανερχόμαστε με tips, tricks, καθώς και πλήρη άρθρα. Έως τότε, εξερευνήστε τις δυνατότητες του Nextcloud και χαρείτε το σε καθημερινή βάση.

Apache, virtual hosts και πιστοποιητικό από Let's Encrypt

Αναλυτικά και βήμα προς βήμα δείχνουμε πώς εγκαθιστούμε και ρυθμίζουμε τον Apache web server σε ένα VPS με openSUSE, καθώς και πώς αποκτάμε έγκυρα πιστοποιητικά SSL για τα virtual hosts του Apache.

Την όλη διαδικασία έχουμε παρουσιάσει για ένα Raspberry Pi με Raspbian, το οποίο δεν έχουμε στο cloud αλλά στο σπίτι μας (https://deltahacker.gr/?p=17024). Αυτή τη φορά στρέφουμε την προσοχή μας σε έναν server στο cloud, ο οποίος τρέχει openSUSE Leap 42.2. Αν και η γενική λογική που ακολουθείται είναι παρόμοια με την περίπτωση του Raspbian, οι λεπτομέρειες της υλοποίησης διαφέρουν αρκετά και συνεπώς το παρόν άρθρο κρίνεται απαραίτητο. Πριν ξεκινήσουμε, ας δούμε τη λίστα με τα προαπαιτούμενα.

- Χρειαζόμαστε ένα **VPS στο cloud που τρέχει openSUSE Leap 42.2.** Αν είστε στην αναζήτηση για ένα τέτοιο VPS, ίσως αξίζει να δείτε την περίπτωση της γερμανικής Hetzner (βλ., π.χ., https://deltahacker.gr/?p=16962 και https://deltahacker.gr/?p=17003).
- Στη γραμμή εντολών του VPS έχουμε **απομακρυσμένη πρόσβαση μέσω SSH**, είτε απευθείας στο λογαριασμό του root είτε σε λογαριασμό άλλου χρήστη που έχει δυνατότητα εκτέλεσης εντολών ως root (π.χ., με τη βοήθεια του sudo).
- Διαθέτουμε **το δικό μας domain name**, καθώς και **πρόσβαση στον name server** που το φιλοξενεί. Σ' αυτόν, υπάρχει ένα A record που αντιστοιχίζει το domain ή κάποιο subdomain του domain στο (δημόσιο) IP του VPS. Το domain που χρησιμοποιήσαμε για τις ανάγκες της παρουσίασης είναι το colder.xyz και, πιο συγκεκριμένα, στον DNS server υπάρχει ένα A record που αντιστοιχίζει το vatnajokull.colder.xyz στο δημόσιο IP του VPS με το openSUSE. Παρεμπιπτόντως, ιδού ένας τρόπος για να μαθαίνουμε το δημόσιο IP του VPS μας:

```
sub0@vatnajokull:~> dig +short myip.opendns.com @resolver1.opendns.com
```

- **Τα ports 80/TCP και 443/TCP του firewall πρέπει να είναι ανοικτά**. Μετά την εγκατάσταση του Apache θα καταφύγουμε στο σχετικό module του YaST, ώστε ν' ανοίξουμε τα προαναφερθέντα ports.
- **Το openSUSE Leap πρέπει να είναι ενημερωμένο:**

  ```
  sub0@vatnajokull:~> sudo zypper ref
  sub0@vatnajokull:~> sudo zypper lu
  sub0@vatnajokull:~> sudo zypper patch
  ```

  Στην περίπτωση που υπάρχει αναβάθμιση για το ίδιο το zypper, θα εμφανιστεί σχετικό μήνυμα και την εντολή sudo zypper patch θα τη δώσουμε ξανά. Επίσης, αν αναβαθμιστεί ο πυρήνας τότε θα χρειαστεί και μια επανεκκίνηση του συστήματος (sudo reboot).
- **Προαιρετικό:** Αν ο provider παρέχει τη δυνατότητα για λήψη snapshots, καλό είναι να δημιουργήσουμε ένα πριν πιάσουμε δουλειά. Έτσι, ακόμη κι αν κάνουμε σειρά από λάθη και μπερδευτούμε, ανά πάσα στιγμή θα μπορούμε να γυρίσουμε το VPS σε μια πρότερη καλή κατάσταση.

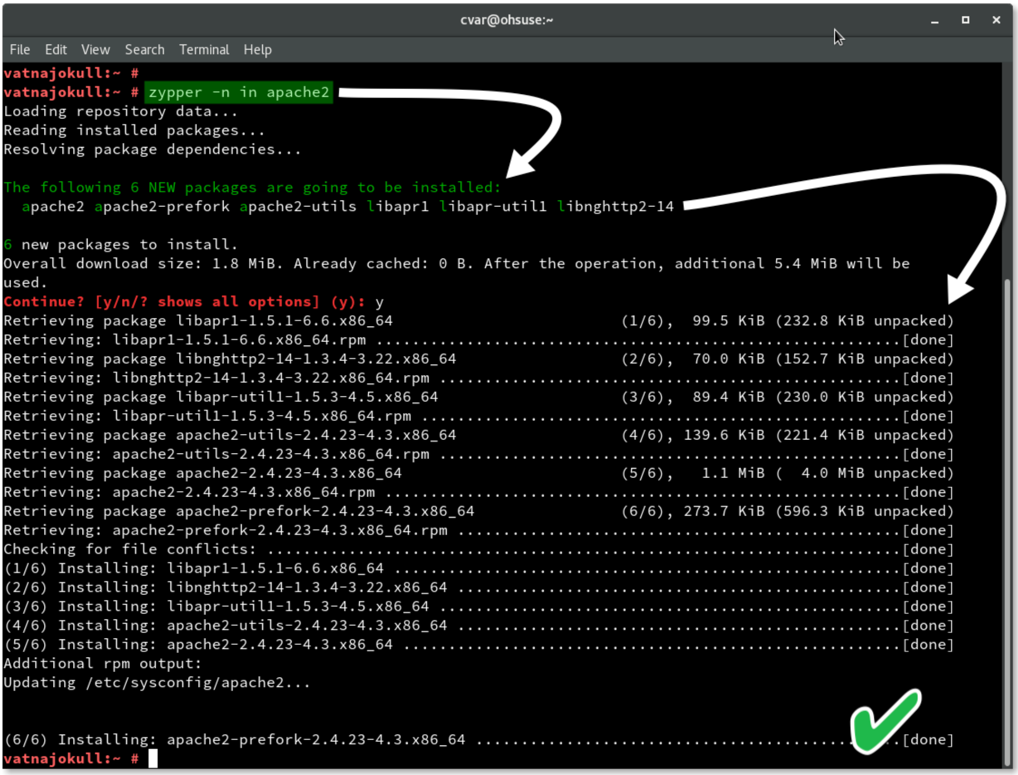
Εγκατάσταση Apache

Για λόγους ασφαλείας δεν επιτρέπουμε στο VPS μας το SSH login στο λογαριασμό του root. Έχουμε βεβαίως ένα λογαριασμό απλού χρήστη, ο οποίος έχει δυνατότητα για εκτέλεση εντολών διαχειριστή μέσω του εργαλείου sudo. Για ακόμη περισσότερη ευκολία, θα μεταβούμε τώρα στο λογαριασμό του root ώστε να εργαστούμε από εκεί:

```
sub0@vatnajokull:~> sudo su
vatnajokull:/home/sub0 # cd
vatnajokull:~ #
```

Η εγκατάσταση του Apache γίνεται με τον αναμενόμενο τρόπο:

```
vatnajokull:~ # zypper -n in apache2
```



Η εξαιρετικά απλή διαδικασία της εγκατάστασης του Apache web server κι όλων των εξαρτήσεών του, στο openSUSE Leap.

Αμέσως μετά την εγκατάστασή του, ο Apache είναι ανενεργός (inactive):

```
vatnajokull:~ # systemctl status apache2.service
• apache2.service - The Apache Webserver
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; vendor
           preset: disabled)
   Active: inactive (dead)
```

Η ενεργοποίηση γίνεται γράφοντας

```
vatnajokull:~ # systemctl start apache2.service
```

Ελέγχοντας ξανά την κατάσταση του Apache, βλέπουμε ότι τώρα είναι πράγματι ενεργός (active) αλλά η υπηρεσία παραμένει απενεργοποιημένη (disabled):

```
vatnajokull:~ # systemctl status apache2.service
• apache2.service - The Apache Webserver
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; vendor
           preset: disabled)
   Active: active (running) since Sun 2017-01-15 20:41:52 CET; 50s ago
 Main PID: 4057 (httpd-prefork)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:   0 B/sec"
    Tasks: 6

[...]

Jan 15 20:41:51 vatnajokull systemd[1]: Starting The Apache Webserver...
Jan 15 20:41:52 vatnajokull systemd[1]: Started The Apache Webserver.
```

Η ενεργοποίηση της υπηρεσίας γίνεται δίνοντας

```
vatnajokull:~ # sudo systemctl enable apache2.service
Created symlink from /etc/systemd/system/httpd.service to /usr/lib/systemd/
system/apache2.service.
Created symlink from /etc/systemd/system/apache.service to /usr/lib/systemd/
system/apache2.service.
Created symlink from /etc/systemd/system/multi-user.target.wants/apache2.
service to /usr/lib/systemd/system/apache2.service.
```

Σημείωση. Αν δεν γνωρίζετε τη διαφορά μεταξύ ενεργοποιημένης κι ενεργής καθώς και τη διαφορά μεταξύ απενεργοποιημένης κι ανενεργής υπηρεσίας, διαβάστε το σχετικό μας άρθρο περί του Systemd (https://deltahacker.gr/?p=16816).

Πρώτες δοκιμές για τον Apache

Τώρα που ο Apache είναι ενεργός (κι ενεργοποιημένος :)) θα θέλαμε να δούμε αν δουλεύει σωστά, δηλαδή αν σερβίρει κάποια προκαθορισμένη σελίδα Ή Κάτι Τέτοιο (ΤΜ). Θα ξεκινήσουμε τους ελέγχους μας πρώτα μέσα από το VPS, με τη βοήθεια ενός browser για την κονσόλα απλού κειμένου και με επίσκεψη στο http://localhost. Μετά θα κάνουμε κι ένα τεστ εξωτερικά, από τον web browser ενός οποιουδήποτε άλλου υπολογιστή και με επίσκεψη στο http://vatnajokull.colder.xyz. Ξεκινάμε από την κονσόλα και με τον browser ονόματι elinks. Αν δεν είναι εγκατεστημένος, το φροντίζουμε αμέσως:

```
vatnajokull:~ # zypper -n in elinks
```

Αμέσως μετά επισκεπτόμαστε το http://localhost γράφοντας

```
vatnajokull:~ # elinks http://localhost
```

Περιέργως, παίρνουμε το μήνυμα λάθους "Access Forbidden!" (για να εγκαταλείψετε το elinks πατήστε το πλήκτρο [Q] και μετά το [Enter]).



Δεν μπορούμε καν ν' ανοίξουμε τη σελίδα καλωσορίσματος του Apache από το localhost;! Χμ, σαν να μην αρχίζουμε καλά... :/

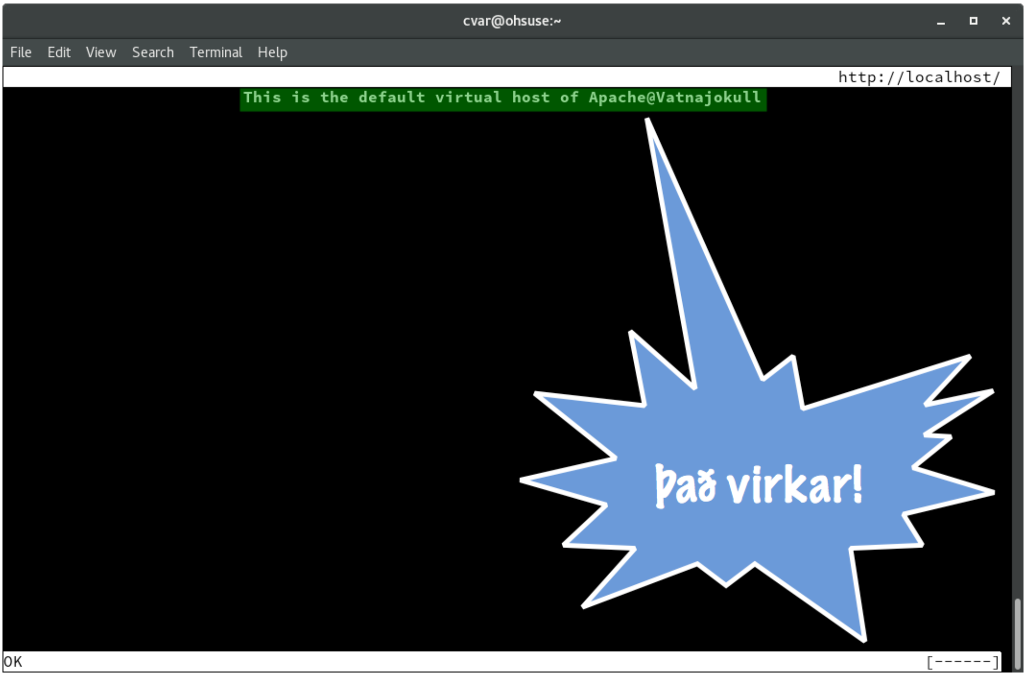
Στο openSUSE, ο κατάλογος στον οποίο βρίσκεται το περιεχόμενο (DocumentRoot) του προκαθορισμένου site (virtual host) του Apache, είναι το /srv/www/htdocs. Πράγματι:

```
vatnajokull:~ # apachectl -S
VirtualHost configuration:
ServerRoot: "/srv/www"
Main DocumentRoot: "/srv/www/htdocs"
Main ErrorLog: "/var/log/apache2/error_log"
Mutex ssl-stapling-refresh: using_defaults
```

```
Mutex ssl-stapling: using_defaults
Mutex ssl-cache: using_defaults
Mutex default: dir="/run/" mechanism=default
Mutex mpm-accept: using_defaults
PidFile: "/run/httpd.pid"
Define: DUMP_VHOSTS
Define: DUMP_RUN_CFG
User: name="wwwrun" id=30
Group: name="www" id=8
```

Αν ρίξουμε μια ματιά στον κατάλογο /srv/www/htdocs, θα διαπιστώσουμε ότι είναι κενός:

```
vatnajokull:~ # ls -lha /srv/www/htdocs
total 8.0K
drwxr-xr-x 2 root root 4.0K Oct  7 17:51 .
drwxr-xr-x 4 root root 4.0K Oct  7 17:51 ..
```



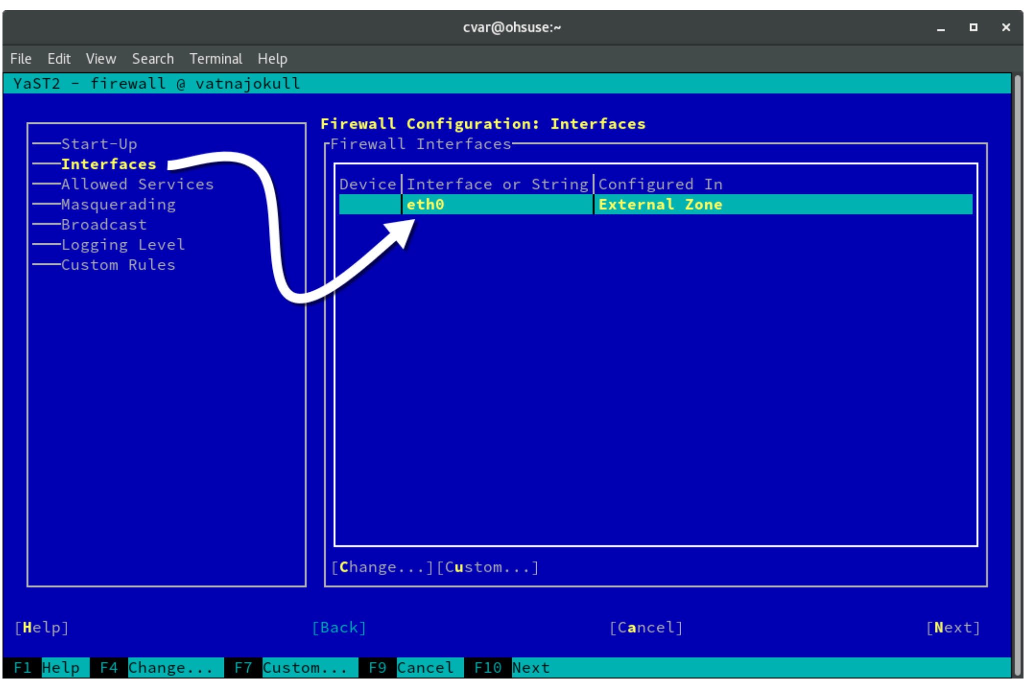
*Ο Apache ακούει για αιτήσεις πελατών *και* από το localhost interface, κι αυτό είναι κάτι που το επαληθεύουμε, π.χ., με τη βοήθεια του elinks.*

Για λόγους ασφαλείας ο Apache δεν επιτρέπει το navigation στο DocumentRoot, έτσι παίρνουμε το μήνυμα λάθους που είδαμε πριν λίγο. Ας φτιάξουμε ένα απλό αρχείο HTML μέσα στο DocumentRoot:

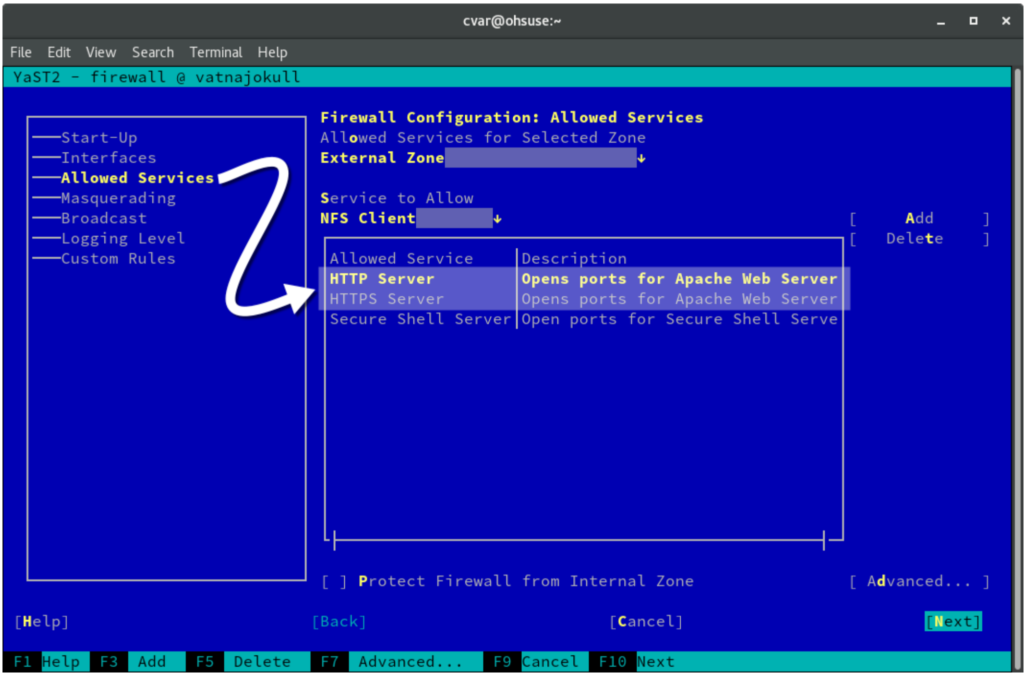
```
vatnajokull:~ # echo '<html><body><h1>This is the default virtual host of
Apache@Vatnajokull</h1></body></html>' > /srv/www/htdocs/index.html
```

Αυτή τη φορά η μετάβαση με το elinks στο http://localhost δεν θα επιστρέψει κάποιο μήνυμα λάθους, αλλά εκείνο που περιλαμβάνεται ανάμεσα στο <h1>...</h1>.

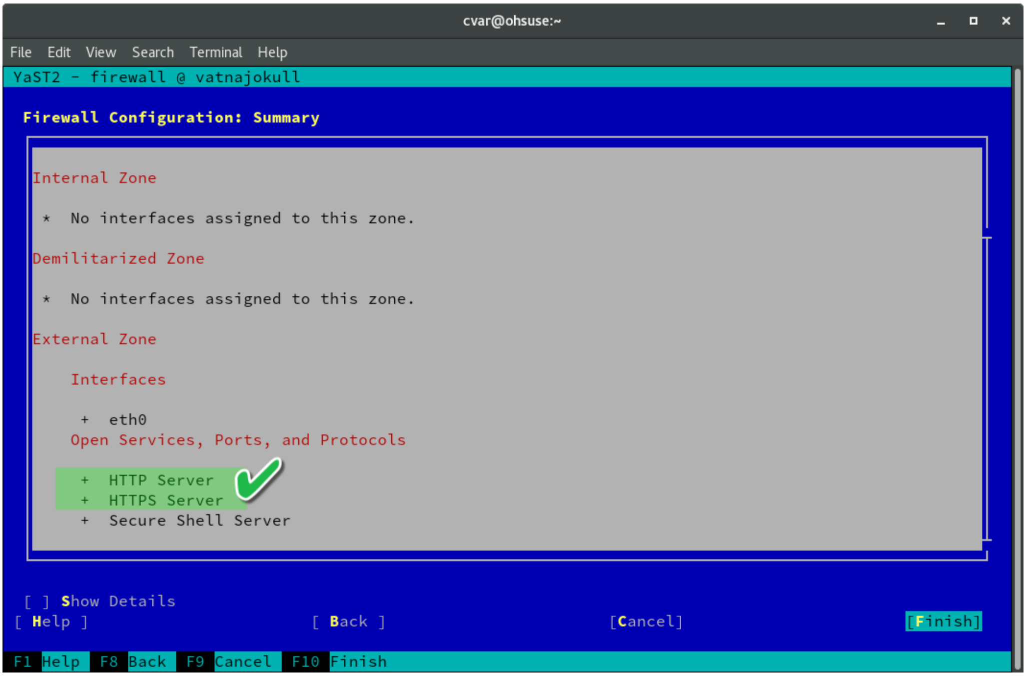
Στη συνέχεια, όμως, επιχειρώντας να επισκεφτούμε το http://vatnajokull.colder.xyz από τον web browser ενός οποιουδήποτε υπολογιστή, διαπιστώνουμε ότι η σύνδεση με τον απομακρυσμένο web server (δηλαδή με τον Apache) δεν προχωρά. Η αποτυχία είναι αναμενόμενη κι οφείλεται στο firewall του openSUSE, το οποίο εξ ορισμού έχει το port 80/TCP κλειστό για το external zone. Φορτώνουμε λοιπόν το module ονόματι "firewall" του YaST (yast2 firewall) και φροντίζουμε ώστε το port 80/TCP να είναι ανοικτό. Και μιας μια κι που αργότερα θα θέλουμε πρόσβαση και στο port 443/TCP, για τις συνδέσεις HTTPS, το ανοίγουμε κι αυτό από τώρα. Δείτε τα screenshots που ακολουθούν, διαβάστε και τις αντίστοιχες περιγραφές.



Το eth0 interface του openSUSE VPS ανήκει στο λεγόμενο external zone. Σε λίγο θα πούμε στο firewall να επιτρέπει τις εισερχόμενες συνδέσεις στο port 80/TCP, για τα interfaces του προαναφερθέντος zone.

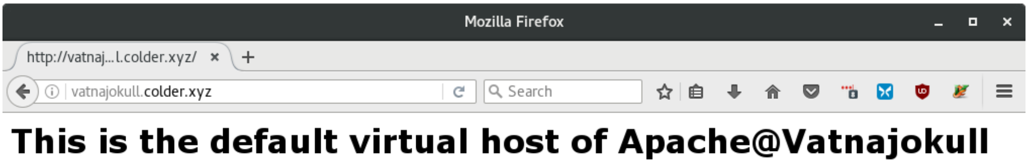


Για το external zone επιτρέπονταν οι εισερχόμενες συνδέσεις προς το port 22/TCP (OpenSSH service), αλλά τώρα φροντίζουμε ώστε να επιτρέπονται και οι εισερχόμενες συνδέσεις προς τα ports 80/TCP και 443/TCP (HTTP και HTTPS αντίστοιχα).



Σύνοψη των αλλαγών που πρόκειται να γίνουν στο σύνολο κανόνων του firewall.

Μετά τις αλλαγές στο firewall, επιχειρώντας να μεταβούμε στο http://vatnajokull.colder.xyz από τον web browser ενός οποιοδήποτε υπολογιστή, βλέπουμε το τυπικό μήνυμα που έχουμε συμπεριλάβει στο index.html. Όλα καλά.



Μετά τις αλλαγές στο firewall του openSUSE μας, από έναν οποιονδήποτε άλλο υπολογιστή βλέπουμε την απλή σελίδα του προκαθορισμένου virtual host που σερβίρει ο Apache.

Τα virtual hosts του Apache

Ο Apache έχει τη δυνατότητα να διαχειρίζεται περισσότερα από ένα sites, τα οποία βρίσκονται όλα τους στο ίδιο φυσικό ή εικονικό μηχάνημα. Για τον Apache, καθένα απ' αυτά τα sites είναι ένας διαφορετικός virtual host και περιγράφεται σε κάποιο configuration file, με κατάληξη *.conf. Οι clients του Apache φτάνουν στα sites που σερβίρει πληκτρολογώντας:

- ένα όνομα, όπως, π.χ., deltahacker.gr, vatnajokull.colder.xyz κ.ο.κ.
- την κατάλληλη αριθμητική διεύθυνση IP (σπάνια στις μέρες μας)
- έναν συνδυασμό ονόματος/IP και port (επίσης σπάνια στις μέρες μας).

Στο παρόν άρθρο μάς ενδιαφέρει κυρίως η πλευρά του server, οπότε ας στρέψουμε την προσοχή μας στον Apache. Πληκτρολογώντας, λοιπόν, `apachectl -S`, παίρνουμε κάποιες πληροφορίες για τον προκαθορισμένο virtual host που υφίσταται αμέσως μετά την εγκατάσταση της υπηρεσίας. Οι παράμετροι που βλέπουμε δεν έχουν σημασία αυτή τη στιγμή. Θα πούμε μόνο ότι το σχετικό αρχείο ρυθμίσεων είναι το default-server.conf, μέσα στον κατάλογο /etc/apache2. Τώρα, η ενδεδειγμένη πρακτική θέλει τα configuration files των virtual hosts να βρίσκονται μέσα στον κατάλογο /etc/apache2/vhosts.d. Ακόμη κι αν έχουμε *μόνο* έναν virtual host, για λόγους καλής διαχείρισης προτείνεται να μη βασιστούμε στο default-server.conf αλλά να δημιουργήσουμε ένα νέο αρχείο *μέσα* στον κατάλογο vhosts.d. Προσέξτε επίσης μια λεπτομέρεια: περισσότερα από ένα virtual hosts είναι δυνατό να περιγράφονται σε *ένα* configuration file. Ξανά όμως για λόγους καλής διαχείρισης, καλό είναι να φροντίζουμε ώστε διαφορετικοί virtual hosts να περιγράφονται σε διαφορετικά configuration files.

Συνοψίζοντας: Κάθε virtual host πρέπει να έχει το δικό του configuration file, το οποίο είναι ένα αρχείο με κατάληξη *.conf και βρίσκεται κάτω από το /etc/apache2/vhosts.d. Όλα, μα όλα, τα αρχεία εντός του συγκεκριμένου καταλόγου που έχουν κατάληξη *.conf, φορτώνονται από τον Apache.

Δημιουργία virtual host για HTTP

Στο openSUSE, μέσα στον κατάλογο /etc/apache2/vhosts.d υπάρχουν τα αρχεία vhost.template και vhost-ssl.template. Όπως φανερώνουν τα ονόματά τους, αποτελούν πρότυπα για τη σύνταξη virtual host configuration files. Είναι φανερό ότι το πρώτο βοηθά στη σύνταξη configuration files για HTTP sites, ενώ το δεύτερο βοηθά στη σύνταξη configuration files για HTTPS sites. Μπορείτε φυσικά να τα αντιγράψετε και να τα μετονομάσετε και να τα τροποποιήσετε καταλλήλως. Για αρχή πάντως, εμείς προτείνουμε κάτι πολύ πιο απλό.

Ξεκινάμε με τη δημιουργία καταλόγων για τη φιλοξενία των αρχείων του site μας, καθώς και των αντίστοιχων αρχείων καταγραφής (log files):

```
vatnajokull:~ # mkdir -p /srv/www/vatnajokull.colder.xyz/{content,logs}
```

Κάτω από τον /srv/www φτιάξαμε τον κατάλογο vatnajokull.colder.xyz, ο οποίος σκόπιμα έχει το πλήρες όνομα του site. Εντός αυτού δημιουργήσαμε και τους καταλόγους content και logs: στον πρώτο θα βρίσκονται όλα τα αρχεία του site, ενώ στον δεύτερο τα log files που θα τηρεί ο Apache για το *συγκεκριμένο* site. Ας φτιάξουμε μέσα στον κατάλογο content ένα απλό αρχείο html, ώστε σε λίγο να μπορέσουμε να κάνουμε και τις δοκιμές μας:

```
vatnajokull:~ # echo '<html><body><h1>Welcome to vatnajokull.colder.xyz!</h1></
body></html>' > /srv/www/vatnajokull.colder.xyz/content/index.html
```

Ωραία. Στο openSUSE μας υπάρχει ένας λογαριασμός απλού χρήστη, με username το sub0. Οι απλοί χρήστες στο openSUSE εξ ορισμού ανήκουν στην ομάδα users. Θέλουμε το περιεχόμενο του vatnajokull.colder.xyz να το διαχειρίζεται ο απλός μας χρήστης, οπότε πριν συνεχίσουμε ας φροντίσουμε για το ιδιοκτησιακό καθεστώς του καταλόγου content κι όλων των περιεχομένων του:

```
vatnajokull:~ # chown -R sub0:users /srv/www/vatnajokull.colder.xyz/content
```

Έχει έρθει η στιγμή να συντάξουμε το configuration file για τον virtual host του vatnajokull.colder.xyz. Το σχετικό αρχείο θα το ονομάσουμε vatnajokull.colder.xyz.conf και θα βρίσκεται εντός του καταλόγου /etc/apache2/vhosts.d. Το δημιουργούμε με τον αγαπημένο μας text editor…

```
vatnajokull:~ # vi /etc/apache2/vhosts.d/vatnajokull.colder.xyz.conf
```

και φροντίζουμε ώστε να περιλαμβάνει το ακόλουθο περιεχόμενο:

```
<VirtualHost *:80>
        ServerName vatnajokull.colder.xyz
        ServerAdmin talk2us@colder.xyz
        DocumentRoot /srv/www/vatnajokull.colder.xyz/content
        ErrorLog /srv/www/vatnajokull.colder.xyz/logs/error.log
        CustomLog /srv/www/vatnajokull.colder.xyz/logs/access.log combined
        <Directory "/srv/www/vatnajokull.colder.xyz/content">
           Require all granted
        </Directory>
</VirtualHost>
```

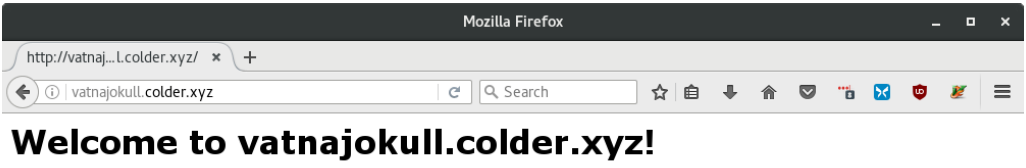
Νομίζουμε ότι η σημασία των οδηγιών είναι προφανής. Αποθηκεύουμε τις αλλαγές στο vatnajokull.colder.xyz.conf κι επανεκκινούμε τον Apache:

```
vatnajokull:~ # systemctl restart apache2.service
```

Αν όλα έχουν πάει καλά, π.χ., δεν υπάρχει κάποιο συντακτικό λάθος στο vatnajokull.colder.xyz.conf, τότε από έναν οποιονδήποτε web browser θα μπορούμε να πηγαίνουμε στο http://vatnajokull.colder.xyz κι εκεί θα βλέπουμε μια λευκή σελίδα με το μήνυμα " Welcome to vatnajokull.colder.xyz!". Κάθε επίσκεψη θα καταγράφεται στο αρχείο access.log, μέσα στον κατάλογο /srv/www/vatnajokull.colder.xyz/logs.



Το απλό configuration file του virtual host που φτιάξαμε για το vatnajokull.colder.xyz. Πολλά περισσότερα για τη σύνταξη των σχετικών αρχείων μπορείτε να διαβάσετε στο επίσημο documentation του Apache, στο https://httpd.apache.org/docs/2.4/vhosts.



Αφού επανεκκινήσουμε τον Apache, ώστε να λάβει υπόψη το νέο virtual host, μια σύντομη δοκιμή από έναν οποιονδήποτε web browser ενός οποιουδήποτε υπολογιστή είναι επιβεβλημένη.

Λήψη κι εγκατάσταση πιστοποιητικού από Let's Encrypt

Θα φτιάξουμε σε πολύ λίγο ένα νέο virtual host, για τις συνδέσεις HTTPS. Αν το αντίστοιχο site είναι πειραματικό ή/και προορίζεται μόνο για χρήση εντός του τοπικού δικτύου, τότε χωρίς πρόβλημα μπορούμε να του έχουμε ένα self-signed πιστοποιητικό. Σε περίπτωση όμως που το site θα είναι προσβάσιμο από το Internet, ένα τέτοιο πιστοποιητικό αν μη τι άλλο θα προβληματίζει τους επισκέπτες. Αντί λοιπόν για self-signed πιστοποιητικό, θα εγκαταστήσουμε ένα έγκυρο που θα είναι υπογεγραμμένο από την Αρχή Πιστοποίησης του Let's Encrypt πρότζεκτ (https://letsencrypt.org).

Χρειαζόμαστε το certbot (https://certbot.eff.org), τον επίσημο client του EFF (https://www.eff.org) για το Let's Encrypt. Το certbot ελέγχει αν είμαστε οι κάτοχοι ενός (sub)domain και στη συνέχεια κατεβάζει κι εγκαθιστά ένα υπογεγραμμένο πιστοποιητικό για το ίδιο (sub)domain (https://certbot.eff.org/about). Δεν υπάρχει πακέτο RPM με το certbot για το openSUSE, μπορούμε ωστόσο να το πάρουμε απευθείας:

```
vatnajokull:~ # wget https://dl.eff.org/certbot-auto
--2017-01-24 06:52:38--  https://dl.eff.org/certbot-auto
Resolving dl.eff.org (dl.eff.org)... 173.239.79.196
Connecting to dl.eff.org (dl.eff.org)|173.239.79.196|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46237 (45K) [text/plain]
Saving to: ‘certbot-auto’
100%[===================================>] 46,237 280KB/s in 0.2s
2017-01-24 06:52:42 (280 KB/s) - ‘certbot-auto’ saved [46237/46237]
```

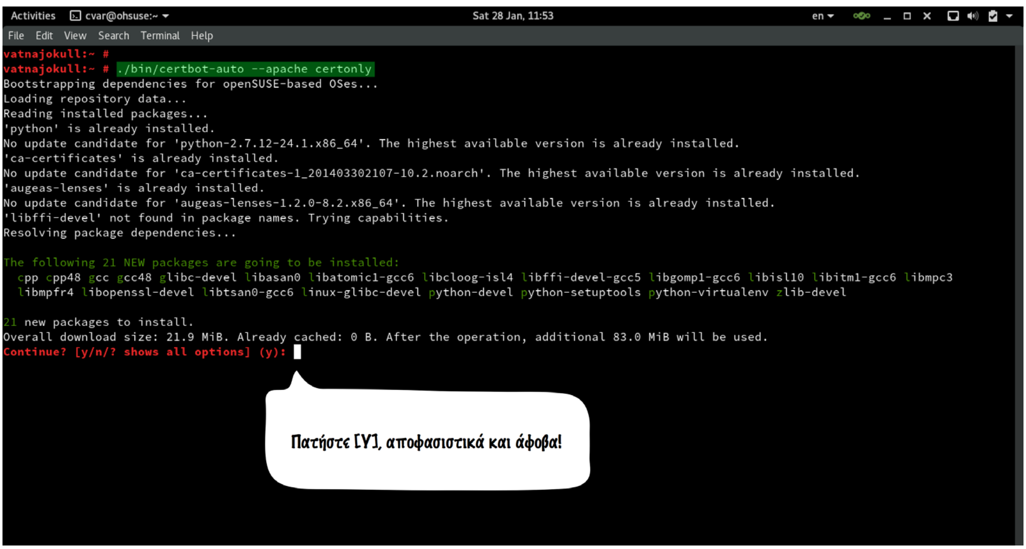
Πρόκειται για το σκριπτάκι certbot-auto, το οποίο μεταφέρουμε στον κατάλογο ~/bin και φροντίζουμε ώστε να είναι εκτελέσιμο:

```
vatnajokull:~ # mv certbot-auto bin/
vatnajokull:~ # chmod +x bin/certbot-auto
```

Αμέσως μετά το τρέχουμε ως ακολούθως:

```
vatnajokull:~ # ./bin/certbot-auto --apache certonly
```

Την πρώτη φορά που το certbot-auto τρέχει σ' ένα σύστημα, ελέγχει για την παρουσία εργαλείων και βιβλιοθηκών που χρειάζεται. Για ό,τι δεν βρίσκει, ζητά άδεια για την εγκατάσταση των αντίστοιχων πακέτων της εκάστοτε διανομής. Εννοείται πως του τη δίνουμε.



Την πρώτη φορά που το certbot-auto τρέχει σ' ένα σύστημα, ελέγχει για την παρουσία εργαλείων και βιβλιοθηκών που χρειάζεται. Για ό,τι δεν βρίσκει, ζητά άδεια για την εγκατάσταση των αντίστοιχων πακέτων για την εκάστοτε διανομή.

Μετά τη λήψη κι εγκατάσταση όλων των απαραίτητων πακέτων που το certbot-auto χρειάζεται για τη λειτουργία του, το script συνεχίζει με τη λήψη και την εγκατάσταση πιστοποιητικών για τους virtual hosts που βρίσκει στο /etc/apache2/vhosts.d. Προσέξτε τα δύο ακόλουθα screenshots, διαβάστε και τις αντίστοιχες περιγραφές.

Θα παρατηρήσατε ίσως ότι πριν λίγο τρέξαμε το certbot-auto με την παράμετρο --apache και την οδηγία certonly. Η παράμετρος --apache σημαίνει ότι για την ταυτοποίηση και την εγκατάσταση, το certbot-only θα χρησιμοποιήσει το plugin για τον Apache (αυτός είναι ο web server που τρέχουμε). Η δε οδηγία certonly λέει στο script να λάβει ή ν' ανανεώσει τα πιστοποιητικά, αλλά να μην επιχειρήσει να δημιουργήσει configuration files για τα αντίστοιχα virtual hosts. Κατά τις δοκιμές μας, αρχικά είχαμε παραλείψει την οδηγία certonly και το certbot-auto απέτυχε να δημιουργήσει configuration file για το vatnajokull.colder.xyz. Σκεφτήκαμε λοιπόν να φτιάξουμε μόνοι μας το αντίστοιχο configuration file. Από τη στιγμή άλλωστε που έχουμε έτοιμο




```
( 7/21) Installing: glibc-devel-2.22-3.7.x86_64 ..............................[done]
( 8/21) Installing: python-virtualenv-13.1.2-2.4.noarch ......................[done]
Additional rpm output:
update-alternatives: using /usr/bin/virtualenv-2.7 to provide /usr/bin/virtualenv (virtualenv) in auto mode


( 9/21) Installing: libcloog-isl4-0.18.1-4.57.x86_64 .........................[done]
(10/21) Installing: libmpc3-1.0.2-4.55.x86_64 ................................[done]
(11/21) Installing: python-devel-2.7.12-24.1.x86_64 ..........................[done]
(12/21) Installing: cpp48-4.8.5-22.1.x86_64 ..................................[done]
(13/21) Installing: cpp-4.8-9.61.x86_64 ......................................[done]
(14/21) Installing: libatomic1-gcc6-6.2.1+r239768-3.3.x86_64 .................[done]
(15/21) Installing: libgomp1-gcc6-6.2.1+r239768-3.3.x86_64 ...................[done]
(16/21) Installing: libitm1-gcc6-6.2.1+r239768-3.3.x86_64 ....................[done]
(17/21) Installing: libtsan0-gcc6-6.2.1+r239768-3.3.x86_64 ...................[done]
(18/21) Installing: zlib-devel-1.2.8-10.1.x86_64 .............................[done]
(19/21) Installing: gcc48-4.8.5-22.1.x86_64 ..................................[done]
(20/21) Installing: libopenssl-devel-1.0.2j-2.2.x86_64 .......................[done]
(21/21) Installing: gcc-4.8-9.61.x86_64 ......................................[done]
Creating virtual environment...
Installing Python packages...
Installation succeeded.
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Enter email address (used for urgent renewal and security notices) (Enter 'c' to
cancel):subZraw@colder.xyz

-------------------------------------------------------------------------------
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.1.1-August-1-2016.pdf. You must agree
in order to register with the ACME server at
https://acme-v01.api.letsencrypt.org/directory
-------------------------------------------------------------------------------
(A)gree/(C)ancel: A

Which names would you like to activate HTTPS for?
-------------------------------------------------------------------------------
1: vatnajokull.colder.xyz
-------------------------------------------------------------------------------
Select the appropriate numbers separated by commas and/or spaces, or leave input
blank to select all options shown (Enter 'c' to cancel):1
```

Μετά το κατέβασμα και την εγκατάσταση των πακέτων που είναι απαραίτητα για τις λειτουργίες του certbot-auto, το script ζητά ένα έγκυρο email (1). Σ' αυτή τη διεύθυνση θα αποστέλλονται ειδοποιήσεις για πιστοποιητικά που πλησιάζουν στη λήξη τους, καθώς και μηνύματα που αφορούν σε ζητήματα ασφαλείας (δεν έχει τύχει να λάβουμε τέτοιο μήνυμα). Στη συνέχεια καλούμαστε να αποδεχτούμε τους όρους χρήσης της υπηρεσίας του Let's Encrypt (2) και μετά καλούμαστε να υποδείξουμε τα domains για τα οποία θέλουμε πιστοποιητικά (3). Εμείς έχουμε έναν μόνο virtual host, αυτόν για το vatnajokull.colder.xyz, οπότε πατάμε [1] και [Enter].




```
Generating key (2048 bits): /etc/letsencrypt/keys/0000_key-certbot.pem
Creating CSR: /etc/letsencrypt/csr/0000_csr-certbot.pem

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at
   /etc/letsencrypt/live/vatnajokull.colder.xyz/fullchain.pem. Your
   cert will expire on 2017-04-28. To obtain a new or tweaked version
   of this certificate in the future, simply run certbot-auto again.
   To non-interactively renew *all* of your certificates, run
   "certbot-auto renew"
 - If you lose your account credentials, you can recover through
   e-mails sent to subZraw@colder.xyz.
 - Your account credentials have been saved in your Certbot
   configuration directory at /etc/letsencrypt. You should make a
   secure backup of this folder now. This configuration directory will
   also contain certificates and private keys obtained by Certbot so
   making regular backups of this folder is ideal.
 - If you like Certbot, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le

vatnajokull:~ #
```

Ακολουθούν μια σειρά από ελέγχους και μετά το certbot-auto κατεβάζει τα αρχεία που συγκροτούν το υπογεγραμμένο πιστοποιητικό για το (sub)domain μας. Όλα είναι καλά, έχουμε όμως λίγη δουλειά ακόμα.

το αντίστοιχο αρχείο για τον HTTP host, η δημιουργία νέου αρχείου για τον HTTPS host δεν είναι δύσκολη υπόθεση. Πράγματι, ξεκινάμε αντιγράφοντας και μετονομάζοντας το vatnajokull.colder.xyz.conf, εντός του καταλόγου /etc/apache2/vhosts.d:

```
vatnajokull:~ # cd /etc/apache2/vhosts.d
vatnajokull:/etc/apache2/vhosts.d # cp vatnajokull.colder.xyz.conf vatnajokull.
colder.xyz-tls-le.conf
```

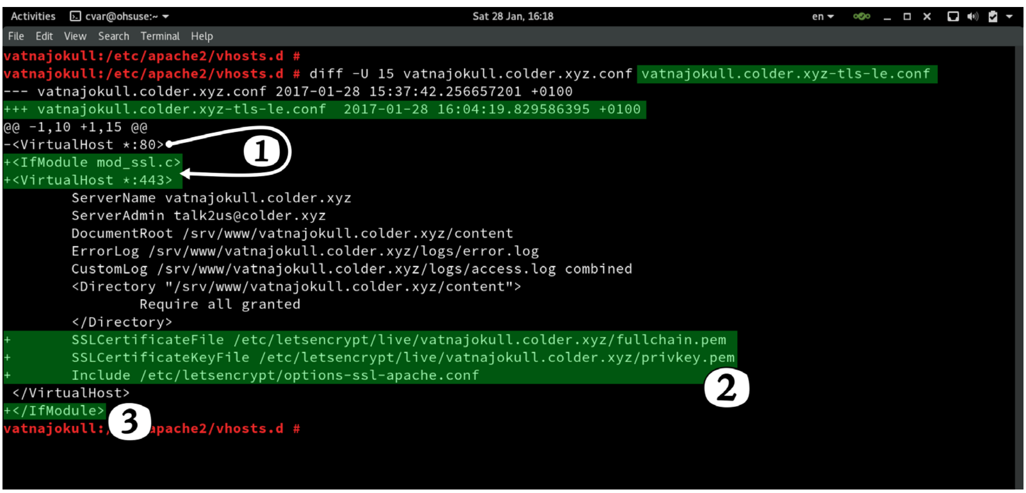
Τροποποιούμε το αρχείο vatnajokull.colder.xyz-tls-le.conf αλλά και του προσθέτουμε νέο περιεχόμενο, ώστε τελικά να μοιάζει με το ακόλουθο:

```
<IfModule mod_ssl.c>
<VirtualHost *:443>
        ServerName vatnajokull.colder.xyz
        ServerAdmin talk2us@colder.xyz
        DocumentRoot /srv/www/vatnajokull.colder.xyz/content
        ErrorLog /srv/www/vatnajokull.colder.xyz/logs/error.log
        CustomLog /srv/www/vatnajokull.colder.xyz/logs/access.log combined
        <Directory "/srv/www/vatnajokull.colder.xyz/content">
                Require all granted
</Directory>
SSLCertificateFile /etc/letsencrypt/live/vatnajokull.colder.xyz/fullchain.pem
SSLCertificateKeyFile /etc/letsencrypt/live/vatnajokull.colder.xyz/privkey.pem
Include /etc/letsencrypt/options-ssl-apache.conf
</VirtualHost>
</IfModule>
```

Ας κάνουμε μια σύνοψη των αλλαγών/προσθηκών στο νέο configuration file (για τον HTTPS host), σε σύγκριση με το "παλιό" configuration file (για τον HTTP host).

- Το μπλοκ ανάμεσα στα <VirtualHost> και </VirtualHost>, το οποίο ορίζει έναν virtual host, τώρα είναι εντεταγμένο ανάμεσα στα <IfModule mod_ssl.c> και </IfModule>. Γενικά, ό,τι περιλαμβάνεται ανάμεσα σε μπλοκ της μορφής <IfModule [!]module_file|module_identifier> ... </IfModule> λαμβάνεται υπόψη ανάλογα με το αποτέλεσμα του ελέγχου για την παρουσία ή την απουσία (!) συγκεκριμένου module του Apache. Στο παράδειγμά μας απλά ελέγχουμε αν το module για την υποστήριξη SSL από πλευράς Apache είναι φορτωμένο. Στο openSUSE φορτώνεται εξ ορισμού κι αυτόματα, επομένως ο έλεγχος είναι αληθής κι ο ορισμός του HTTPS host λαμβάνεται υπόψη από τον web server.
- Ο ορισμός του virtual host για HTTPS ξεκινά με ένα <VirtualHost *:443> κι όχι με ένα <VirtualHost *:80>, αφού εξ ορισμού οι συνδέσεις HTTPS γίνονται στο port 443/TCP.

- Λίγο πριν το τέλος του νέου virtual host έχουν προστεθεί οδηγίες αφενός για το φόρτωμα του cain file (πιστοποιητικό του domain μαζί με το πιστοποιητικό της Αρχής Πιστοποίησης του Let's Encrypt), αφετέρου για το φόρτωμα του ιδιωτικού κλειδιού που αντιστοιχεί στο πιστοποιητικό (περιλαμβάνει το δημόσιο κλειδί) του domain.
- Η τελευταία οδηγία πριν το "κλείσιμο" του virtual host συμπεριλαμβάνει όλες τις οδηγίες που παρατίθενται στο αρχείο /etc/letsencrypt/options-ssl-apache.conf (έχει δημιουργήσει το certbot-auto). Ουσιαστικά, οι οδηγίες του συγκεκριμένου αρχείου ενισχύουν την ασφάλεια και την αξιοπιστία των συνδέσεων HTTPS που υποστηρίζει ο Apache μας.

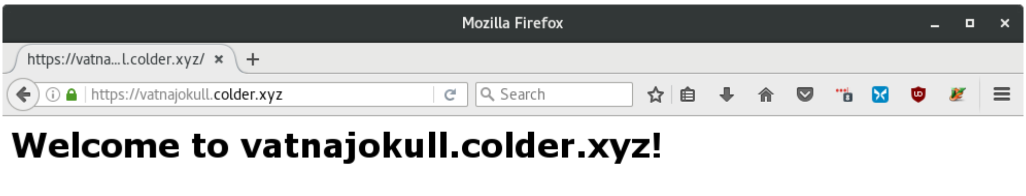


Οι διαφορές στα configuration files των δύο virtual hosts για το vatnajokull.colder.xyz, όπως φαίνονται με τη βοήθεια του εργαλείου diff και με μερικές έξτρα πινελιές :)

Όπως ίσως θα παρατηρήσατε, το certbot-auto έχει τακτοποιήσει πιστοποιητικά και ιδιωτικό κλειδί κάτω από το /etc/letsencrypt/live/vatnajokull.colder.xyz. Στην πραγματικότητα, για κάθε domain αποθηκεύει τα σχετικά αρχεία σε έναν κατάλογο της μορφής /etc/letsencrypt/archive/domain. Κάτω από τους καταλόγους της μορφής /etc/letsencrypt/live/domain υπάρχουν symbolic links προς τις πλέον πρόσφατες εκδόσεις πιστοποιητικών και ιδιωτικών κλειδιών για το εκάστοτε domain. Μην ξεχνάτε ότι μετά από συγκεκριμένο χρονικό διάστημα τα πιστοποιητικά λήγουν, οπότε από τη μεριά μας φροντίζουμε να τ' ανανεώνουμε. Λίγο αργότερα θα δούμε πώς ακριβώς αυτοματοποιούνται οι εν λόγω ανανεώσεις. Προς το παρόν, ας επανεκκινήσουμε τον Apache ώστε να λάβει υπόψη και τον νέο HTTPS host:

```
vatnajokull:~ # systemctl restart apache2.service
```

Αν όλα έχουν πάει καλά, από έναν οποιονδήποτε web browser θα είμαστε σε θέση να επισκεφτούμε τη διεύθυνση https://vatnajokull.colder.xyz (προσοχή στο "s") και θα δούμε το μήνυμα "Welcome to vatnajokull.colder.xyz!". Όλα καλά – ή για την ακρίβεια *σχεδόν* όλα καλά. Έχουμε λίγη ακόμη δουλειά.



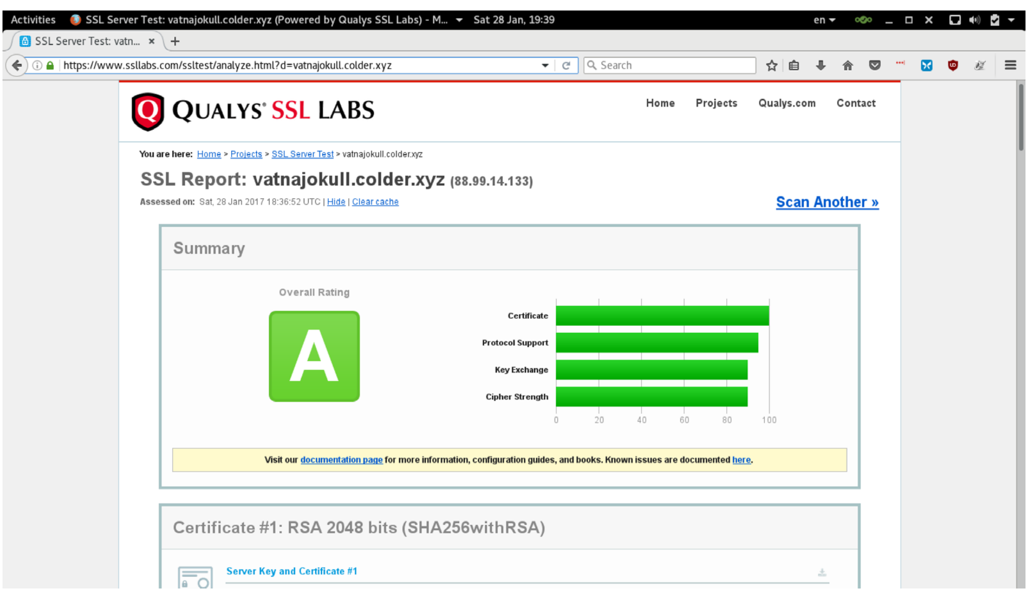
Όπως φαίνεται και με τη βοήθεια του Firefox, ο virtual host για τις συνδέσεις HTTPS προς το vatnajokull.colder.xyz έχει οριστεί σωστά. Υπάρχουν όμως μερικές εκκρεμότητες ακόμα, τις οποίες πρέπει να δούμε.

Δοκιμές και βελτιώσεις

Μετά την εγκατάσταση πιστοποιητικού για ένα domain, είναι πάντα καλή ιδέα να πηγαίνουμε μια βόλτα από το https://www.ssllabs.com και να κάνουμε μια σειρά από ελέγχους για την ποιότητα των συνδέσεων SSL/TSL που υποστηρίζει ο web server. Το απευθείας URL για την άμεση εκκίνηση των ελέγχων μοιάζει με αυτό:

https://www.ssllabs.com/ssltest/analyze.html?d=vatnajokull.colder.xyz&latest

Οι έλεγχοι διαρκούν λίγα λεπτά κι όταν ολοκληρώνονται βλέπουμε, μεταξύ άλλων, τη συνολική μας αξιολόγηση. Για όσα έχουμε κάνει έως τώρα, αυτή θα είναι "A". Δείχνει καλή –και είναι καλή– μπορεί όμως να βελτιωθεί και να πάρουμε "A+".



Αυτό το "A" δεν είναι άσχημο, αλλά εύκολα μπορούμε να το κάνουμε "A+".

Όπως είναι ορισμένοι αυτή τη στιγμή οι δύο virtual hosts για το vatnajokull.colder.xyz (ένας για τις συνδέσεις HTTP κι άλλος ένας για τις συνδέσεις HTTPS), όταν επισκεπτόμαστε τη διεύθυνση http://vatnajokull.colder.xyz *δεν* ανακατευθυνόμαστε αυτόματα, όπως θα μπορούσαμε και θα θέλαμε, στο https://vatnajokull.colder.xyz. Μ' άλλα λόγια, ακόμα κι όταν επιχειρούμε επισφαλή σύνδεση HTTP, αυτομάτως θα πρέπει να γυρνάμε σε ασφαλή σύνδεση HTTPS. Αυτό επιτυγχάνεται πολύ εύκολα, προσθέτοντας στο τέλος του configuration file για τον HTTP virtual host μία μόνο γραμμή:

```
<VirtualHost *:80>
        ServerName vatnajokull.colder.xyz
        ServerAdmin talk2us@colder.xyz
        DocumentRoot /srv/www/vatnajokull.colder.xyz/content
        ErrorLog /srv/www/vatnajokull.colder.xyz/logs/error.log
        CustomLog /srv/www/vatnajokull.colder.xyz/logs/access.log combined
        <Directory "/srv/www/vatnajokull.colder.xyz/content">
                Require all granted
        </Directory>
        Redirect / https://vatnajokull.colder.xyz/
</VirtualHost>
```

Επανεκκινούμε τον Apache...

```
vatnajokull:~ # systemctl restart apache2.service
```

...κι από έναν οποιονδήποτε web browser μεταβαίνουμε στη διεύθυνση http://vatnajokull.colder.xyz. Παρουσία της οδηγίας Redirect, αυτομάτως ανακατευθυνόμαστε στο https://vatnajokull.colder.xyz (προσοχή, ίσως χρειαστεί ένα refresh για τον browser). Πάρα πολύ ωραία, μόνο που η συγκεκριμένη βελτίωση δεν είναι αρκετή για να μας δώσει το SSLLabs "A+".

Προκειμένου λοιπόν να κερδίσουμε το "άριστα", χρειάζεται να δούμε το ζήτημα του HTTP Strict Transport Security (HSTS). Θέτοντας την κατάλληλη τιμή στον HSTS header, διασφαλίζουμε ότι στους επισκέπτες του vatnajokull.colder.xyz *δεν* θα επιτρέπονται απλές συνδέσεις HTTP. Προσέξτε: Αν και αυτή τη στιγμή οι συνδέσεις HTTP προς το vatnajokull.colder.xyz αναβαθμίζονται αυτόματα σε συνδέσεις HTTPS, χωρίς το HSTS header η υλοποίηση επιθέσεων Man-in-The-Middle παραμένει εφικτός κίνδυνος. Για το HSTS, λοιπόν, ανοίγουμε το αρχείο vatnajokull.colder.xyz-tls-le.conf και λίγο πριν το "κλείσιμο" του virtual host προσθέτουμε τρεις νέες γραμμές:

```
<IfModule mod_ssl.c>
<VirtualHost *:443>
        ServerName vatnajokull.colder.xyz
        ServerAdmin talk2us@colder.xyz
        DocumentRoot /srv/www/vatnajokull.colder.xyz/content
        ErrorLog /srv/www/vatnajokull.colder.xyz/logs/error.log
        CustomLog /srv/www/vatnajokull.colder.xyz/logs/access.log combined
        <Directory "/srv/www/vatnajokull.colder.xyz/content">
                Require all granted
        </Directory>
        SSLCertificateFile /etc/letsencrypt/live/vatnajokull.colder.xyz/
fullchain.pem
        SSLCertificateKeyFile /etc/letsencrypt/live/vatnajokull.colder.xyz/
privkey.pem
        Include /etc/letsencrypt/options-ssl-apache.conf
        <IfModule mod_headers.c>
                Header always set Strict-Transport-Security "max-age=15552000;
includeSubDomains; preload"
        </IfModule>
</VirtualHost>
</IfModule>
```

Φροντίζουμε αμέσως μετά ώστε το module ονόματι mod_headers να είναι φορτωμένο...

```
vatnajokull:~ # a2enmod mod_headers
```

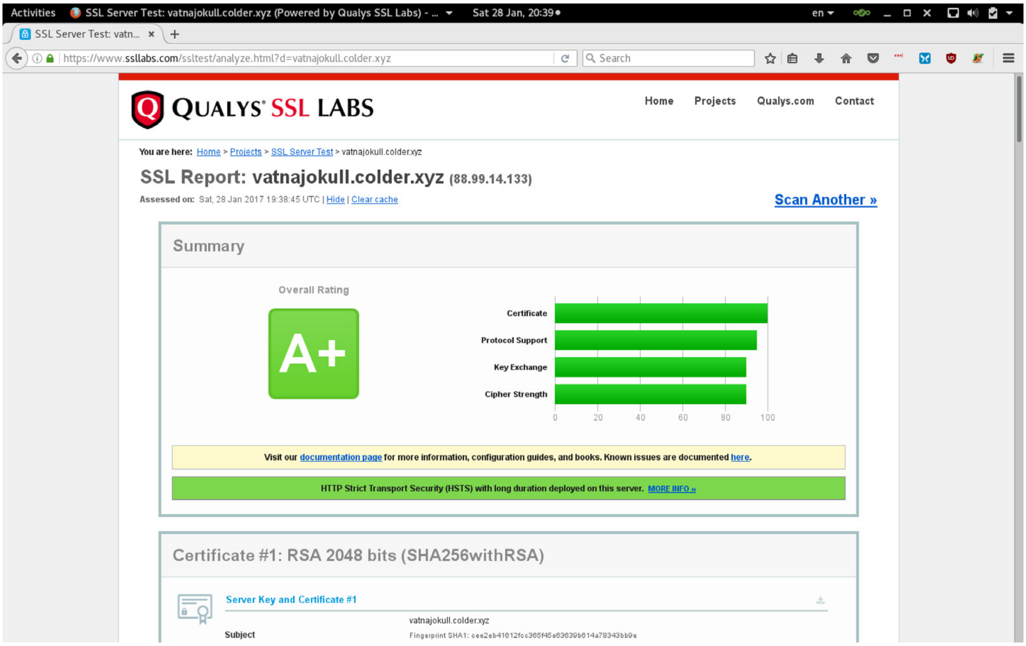
...κι επανεκκινούμε τον Apache ώστε να ληφθούν υπόψη οι αλλαγές για τον HTTPS virtual host:

```
vatnajokull:~ # systemctl status apache2.service
```

Πηγαίνοντας ξανά στο https://www.ssllabs.com και πραγματοποιώντας τους ελέγχους, με πολλή χαρά διαπιστώσουμε ότι η συνολική μας αξιολόγηση πλέον είναι "A+".

Αυτόματη ανανέωση

Τα πιστοποιητικά που εκδίδει το Let's Encrypt διαρκούν για τρεις μήνες. Αν λοιπόν δεν έχουμε φροντίσει για την έγκαιρη ανανέωση του δικού μας, οι επισκέπτες του site θα βλέπουν τη γνωστή, ανησυχητική προειδοποίηση περί ληγμένου πιστοποιη-



Αξιολόγηση "A+" για τις συνδέσεις TLS/SSL που υποστηρίζει ο Apache μας! Extra bonus: Η υλοποίηση επιθέσεων Man-in-The-Middle προς το site μας καθίσταται εξαιρετικά δύσκολη υπόθεση.

τικού. Η ανανέωση των πιστοποιητικών επιτυγχάνεται με τη βοήθεια του certbot-auto. Μπορούμε βεβαίως να φτιάξουμε ένα cronjob για τον root, το οποίο θα φροντίζει γι' αυτή τη δουλειά αυτόματα. Ξεκινάμε πληκτρολογώντας

```
vatnajokull:~ # crontab -e
```

κι αμέσως προσθέτουμε μια νέα εργασία για τον cron daemon. Δείτε το περιεχόμενο του δικού μας crontab:

```
MAILTO = ""
45 6 * * 7 /root/bin/certbot-auto renew
```

Κάθε Κυριακή στις 06:45 το πρωί καλείται το certbot-auto με την εντολή renew. Αν και μόνον αν το πιστοποιητικό μας πλησιάζει στη λήξη του, τότε θα ανανεώνεται αυτόματα. Παρατηρήστε ότι έχουμε πει στον cron daemon να μη στέλνει email κάθε φορά που εκτελείται κάποιο cronjob για τον root. Σε περίπτωση που παρατηρήσουμε ότι κάτι δεν έχει πάει καλά με την ανανέωση θα ανοίξουμε το αρχείο καταγραφής letsencrypt.log, μέσα στον κατάλογο /var/log/letsencrypt. Και μια τελευταία σημείωση: Καλό είναι να βάλετε διαφορετική μέρα και ώρα στο cronjob σας, ώστε να μην πέφτουμε όλοι μαζί πάνω στους servers του Let's Encrypt.

Skill: Beginner
Tags: SSH, public key authentication

Ενεργοποίηση του SSH agent σε terminal sessions

Η προστασία ενός ιδιωτικού κλειδιού SSH με passphrase προτείνεται ενθουσιωδώς όταν μιλάμε για laptop που είναι πιθανό να ξεχάσουμε κάπου ή ακόμη και να κλαπεί. Επίσης, το passphrase είναι έξυπνη κίνηση όταν περισσότεροι από ένας άνθρωποι έχουν πρόσβαση στον ίδιο λογαριασμό χρήστη ή όταν, πολύ απλά, δεν εμπιστευόμαστε το μηχάνημα στο οποίο βρίσκεται αποθηκευμένο κάποιο ιδιωτικό μας κλειδί.

Κάθε φορά που μια εφαρμογή χρειάζεται πρόσβαση σε ιδιωτικό κλειδί SSH κι αυτό είναι προστατευμένο με passphrase (https://deltahacker.gr/?p=16981), αμέσως ζητείται η πληκτρολόγησή του. Με την προϋπόθεση ότι το passphrase δίνεται σωστά, επιτρέπεται η πρόσβαση στο κλειδί.

Σε συστήματα Linux με σύγχρονο περιβάλλον γραφικών όπως, π.χ., είναι το GNOME, για τη διευκόλυνση του χρήστη ενεργοποιείται ο λεγόμενος ssh-agent. Χάρη σ' αυτό το εργαλείο, το ιδιωτικό κλειδί παραμένει στη μνήμη καθ' όλη τη διάρκεια της τρέχουσας συνεδρίας (session) κι ο agent αναλαμβάνει εκείνος το public key authentication για λογαριασμό άλλων εφαρμογών. Πρακτικά, λοιπόν, δεν χρειάζεται να πληκτρολογούμε τόσο συχνά το passphrase ενός ιδιωτικού κλειδιού. Πέρα από την ευκολία, η άμεση πρόσβαση σε ένα ιδιωτικό κλειδί SSH, δηλαδή η πρόσβαση σ' αυτό χωρίς την πληκτρολόγηση passphrase, είναι απαραίτητη προϋπόθεση για την ορθή λειτουργία scripts τα οποία προϋποθέτουν ότι οι συνδέσεις SSH προς άλλα hosts γίνονται χωρίς να ζητείται password ή passphrase.

Η κατάσταση είναι ελαφρώς διαφορετική όταν συνδεόμαστε στην κονσόλα τερματικού ενός απομακρυσμένου μηχανήματος Linux, αφού τότε δεν θα φορτωθεί αυτόματα το ssh-agent. Ευτυχώς μπορούμε να το ξεκινήσουμε χειροκίνητα και μετά να του δώσουμε το ιδιωτικό μας κλειδί. Παρακολουθείστε το ακόλουθο σενάριο, δείτε και το συνοδευτικό screenshot.

1. Από τον υπολογιστή μας με hostname το dalvik, συνδεόμαστε σε έναν απομακρυσμένο Linux host με hostname το isafjordur. Η ταυτοποίηση του χρήστη γίνεται με βάση το public key authentication (https://deltahacker.gr/?p=13357). Επειδή στον λογαριασμό μας στο dalvik το ιδιωτικό κλειδί SSH δεν προστατεύεται από passphrase, η σύνδεση στο isafjordur επιτυγχάνεται άμεσα και

```
Virkni   pi@nordostbahnhof: ~                    fim 30. mar, 11:46
Skrá  Breyta  Skoða  Leita  Skjáhermir  Hjálp
cvar@dalvík:~>
cvar@dalvík:~> ssh isafjordur
Last login: Thu Mar 30 11:36:23 2017 from 10.163.0.239
Have a lot of fun...
sub0@ísafjörður:~>
sub0@ísafjörður:~> ssh nue
Enter passphrase for key '/home/sub0/.ssh/id_rsa':

Welcome to this fiiiiine Raspberry Pi!

No mail.
Last login: Thu Mar 30 11:42:32 2017 from charybdis-ext.suse.de
pi@nordostbahnhof:~ $ logout
Connection to nue.colder.xyz closed.
sub0@ísafjörður:~>
sub0@ísafjörður:~> eval $(ssh-agent)
Agent pid 5935
sub0@ísafjörður:~> ssh-add
Enter passphrase for /home/sub0/.ssh/id_rsa:
Identity added: /home/sub0/.ssh/id_rsa (/home/sub0/.ssh/id_rsa)
sub0@ísafjörður:~>
sub0@ísafjörður:~> ssh nue

Welcome to this fiiiiine Raspberry Pi!

No mail.
Last login: Thu Mar 30 11:44:19 2017 from charybdis-ext.suse.de
pi@nordostbahnhof:~ $ logout
Connection to nue.colder.xyz closed.
sub0@ísafjörður:~>
sub0@ísafjörður:~> ssh vatnajokull
Last login: Thu Mar 30 11:42:45 2017 from 195.135.221.2
Have a lot of fun...
sub0@vatnajokull:~> logout
Connection to vatnajokull.colder.xyz closed.
sub0@ísafjörður:~>
```

1 2 3 4 5

*Συνδέσεις μέσω SSH σε απομακρυσμένα hosts, βάσει public key authentication. Όταν το ιδιωτικό μας κλειδί προστατεύεται από passphrase, ένας τρόπος ώστε να *μη χρειάζεται* να το πληκτρολογούμε διαρκώς στο τρέχον terminal session είναι να δώσουμε το κλειδί στον ssh-agent με τη βοήθεια του εργαλείου ssh-add.*

χωρίς να πληκτρολογήσουμε κάτι. [Παρεμπιπτόντως, χάρη στα SSH aliases (https://deltahacker.gr/?p=14040) ξεκινήσαμε τη σύνδεση στο isafjordur πληκτρολογώντας, απλά, ssh isafjordur.]

2. Αργότερα, από το isafjordur θέλουμε να συνδεθούμε –πάντα μέσω SSH– σε ένα Raspberry Pi στο σπίτι, με hostname το nue. Και πάλι η ταυτοποίηση γίνεται με βάση το public key authentication, τώρα όμως το ιδιωτικό μας κλειδί στο isafjordur προστατεύεται με passphrase. Πριν λοιπόν γίνει έλεγχος για το αν επιτρέπεται η σύνδεση στο nue, μας ζητείται η πληκτρολόγηση του εν λόγω passphrase. Το δίνουμε κι όλα προχωρούν κανονικά.
3. Μετά από λίγο αποσυνδεόμαστε από το nue. Σκεφτόμαστε ότι για το υπόλοιπο που θα μείνουμε συνδεδεμένοι στο isafjordur, δεν θα θέλαμε να πληκτρολογήσουμε ξανά το passphrase για το ιδιωτικό κλειδί που έχουμε εκεί. Πρέπει, λοιπόν, να το δώσουμε στον ssh-agent. Ένας *σωστός* τρόπος για να πετύχουμε το σκοπό μας είναι να πληκτρολογήσουμε

   ```
   sub0@ísafjörður:~> eval $(ssh-agent)
   ```

   και μετά

   ```
   sub0@ísafjörður:~> ssh-add
   ```

   Το γιατί τρέξαμε το ssh-agent μέσω του eval θα το δούμε σε λίγο. Προς το παρόν, ας σημειώσουμε ότι με τη βοήθεια του εργαλείου ssh-add πληκτρολογούμε το passphrase του ιδιωτικού μας κλειδιού κι ο ssh-agent το διαβάζει και το κρατά στη μνήμη, για όσο παραμένουμε συνδεδεμένοι στο τρέχον terminal session.
4. Δείτε, τώρα, ότι συνδεόμαστε στο nue χωρίς πληκτρολόγηση passphrase...
5. ...και το ίδιο ισχύει και για συνδέσεις σε άλλα hosts, όπως είναι το vatnajokull, στα οποία έχουμε πρόσβαση μέσω SSH και με public key authentication.

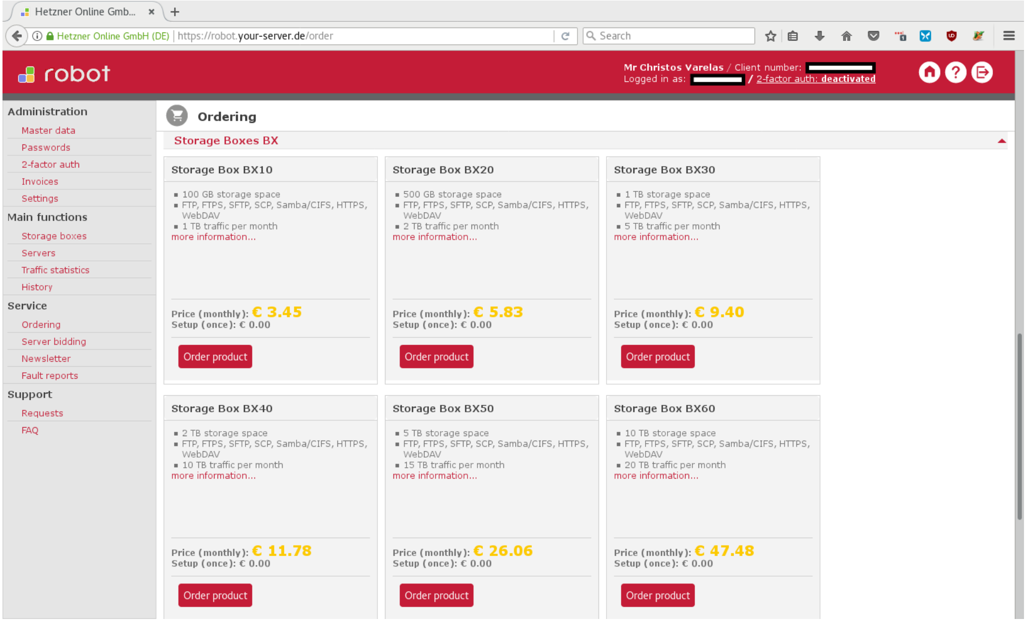
Γιατί δεν τρέξαμε το ssh-agent απευθείας αλλά μέσω του eval; Η απάντηση είναι στο man page του ssh-agent. Με λίγα λόγια, αν ενεργοποιήσουμε το πρόγραμμα πληκτρολογώντας κάτι σαν `ssh-agent bash`, αρχικοποιούνται ορισμένες μεταβλητές περιβάλλοντος οι οποίες περνάνε σε ένα νέο κέλυφος BASH. Σ' αυτό το νέο κέλυφος τρέχουμε το ssh-add, το πρόγραμμα εξετάζει τις τιμές των προαναφερθέντων μεταβλητών και χάρη σ' αυτές μπορεί και δίνει το ιδιωτικό κλειδί στον ssh-agent. Εμείς όμως δεν θέλουμε να ξεκινήσουμε ένα νέο κέλυφος, το παρόν στο οποίο είμαστε συνδεδεμένοι μας κάνει μια χαρά. Ακριβώς γι' αυτό τρέχουμε το ssh-agent μέσω του eval, το οποίο βλέπει τις νέες μεταβλητές που αρχικοποιεί το ssh-agent και τις διατηρεί στο παρόν session. Έτσι, το ssh-add δεν έχει κανένα πρόβλημα επικοινωνίας με το ssh-agent.

Skill: Intermediate
Tags: online storage, WebDAV

Storage box για τον cloud server κι όχι μόνο

Είμαστε βέβαιοι ότι το VPS σας διαθέτει τα χαρακτηριστικά που απαιτούνται για τις δικτυακές σας εφαρμογές, υποψιαζόμαστε όμως ότι ίσως υστερεί σε αποθηκευτικό χώρο. Ευτυχώς αρκετοί providers έχουν αρχίσει να προσφέρουν τη δυνατότητα για αγορά έξτρα χώρου, σε ξεχωριστά δικτυακά volumes.

Ένα τέτοιο volume το προσαρτάτε στον server σας, άσχετα αν αυτός είναι τοπικός ή βρίσκεται κάπου στο cloud. Αν κάποια στιγμή θελήσετε περισσότερο χώρο, εύκολα μπορείτε και να μεγαλώσετε το volume *χωρίς* απώλεια δεδομένων. Είναι ακόμη δυνατό να μικρύνετε το volume, αρκεί βέβαια τα αποθηκευμένα δεδομένα να "χωρούν" στο νέο μέγεθος.

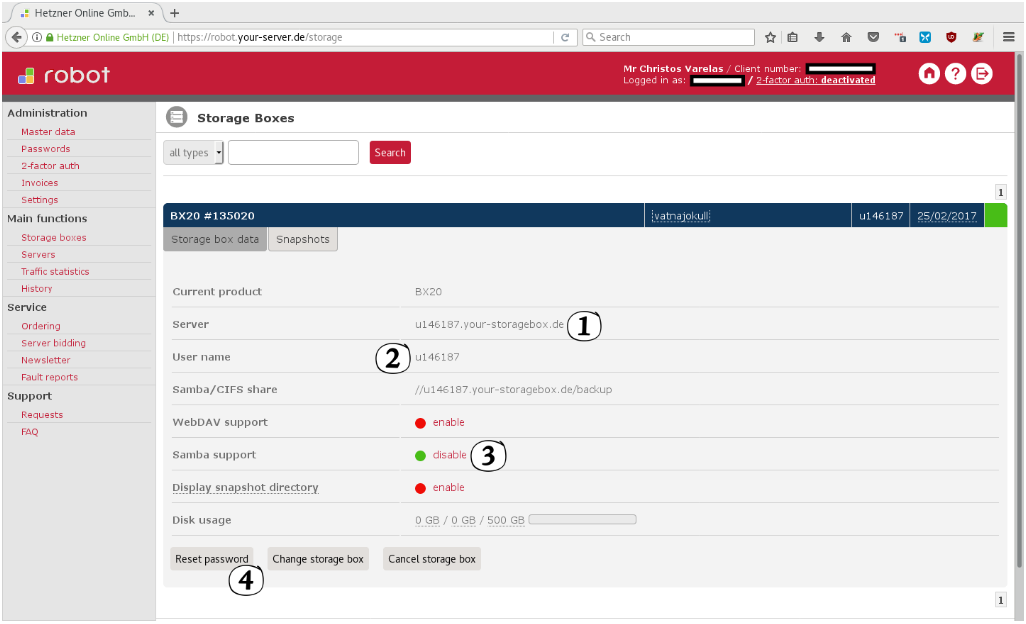


Θα ξεκινούσαμε με ένα Storage Box BX10, όμως ήδη έχουμε γύρω στα 300GB που θέλουμε να μεταφέρουμε στο cloud. Πήραμε λοιπόν ένα Storage Box BX20 γνωρίζοντας ότι α) μετά τη μεταφορά θα μας περισσέψει αρκετός αποθηκευτικός χώρος, β) αν κάποια στιγμή στο μέλλον χρειαστούμε περισσότερο χώρο, τότε πολύ εύκολα θα επεκτείνουμε το Storage Box χωρίς να χάσουμε δεδομένα.

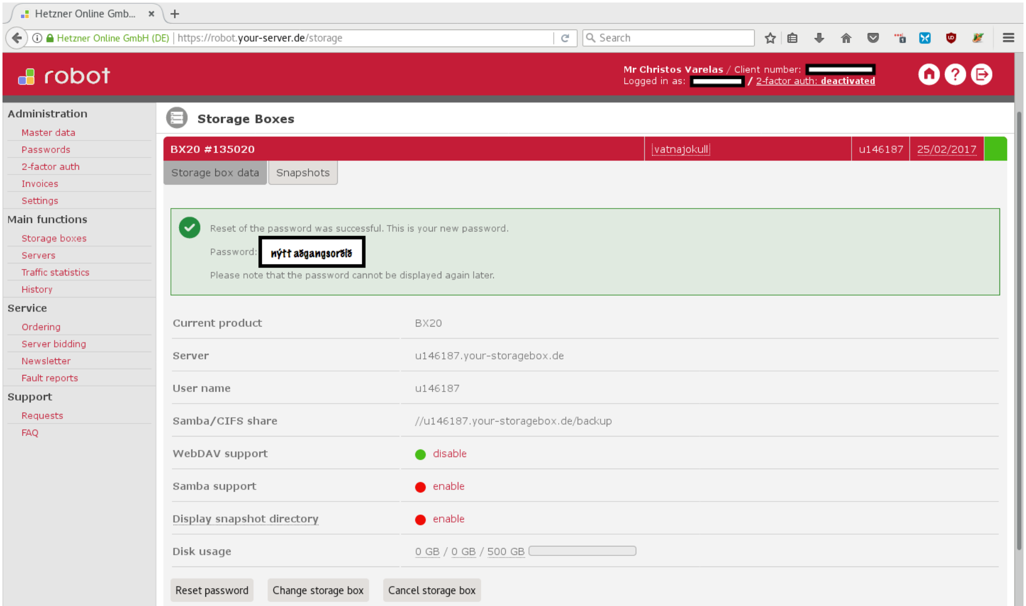
Storage box για τον cloud server κι όχι μόνο

Προσφάτως αγοράσαμε ένα storage volume χωρητικότητας 500GB, το οποίο και προσαρτήσαμε σε ένα VPS με openSUSE Leap 42.2. Ο provider τόσο του VPS όσο και του volume ήταν η Hetzner (https://hetzner.de). Η εταιρεία ονομάζει τα volumes που προσφέρει ως Storage Boxes, με το μικρότερο να ξεκινά από τα 100GB (Storage Box BX10, στα 3,45 ευρώ/μήνα) και το μεγαλύτερο να φτάνει στα 10TB (Storage Box BX60, στα 47,48 ευρώ/μήνα). Όπως ήδη αναφέραμε, εμείς αγοράσαμε ένα Storage Box BX20, στα 5,83 ευρώ/μήνα, αφού ο συνολικός όγκος των δεδομένων που επιθυμούμε να έχουμε εκεί είναι κοντά στα 300GB.

Σημειώστε ότι ένα storage volume μπορείτε να το εκμεταλλευτείτε ακόμη κι αν δεν έχετε μηχάνημα (εικονικό ή φυσικό) με Linux. Στη συνέχεια του παρόντος, ωστόσο, δείχνουμε πώς προσαρτούμε ένα Storage Box σε έναν server με openSUSE Leap 42.2. Ανάλογα θα εργαστείτε αν αντί για openSUSE χρησιμοποιείτε άλλη διανομή του Linux.



Είναι σημαντικό να σημειώσουμε κάπου το πλήρες όνομα (fully qualified domain name, FQDN) του server στον οποίο φιλοξενείται και διατίθεται το volume μας. Στο παράδειγμα, το εν λόγω πλήρες όνομα είναι το u146187. your-storage.box (1). Το δε hostname του server, δηλαδή αυτό το u146187, είναι και το username του λογαριασμού μας εκεί (2). Παρατηρήστε ότι το volume είναι διαθέσιμο μέσω του πρωτοκόλλου CIFS (Samba support, 3). Το συγκεκριμένο πρωτόκολλο βολεύει ιδιαίτερα ειδικά αν σκοπεύουμε να προσαρτήσουμε το volume από μηχάνημα με Windows. Εμείς δεν πρόκειται να κάνουμε κάτι τέτοιο, αφού μας ενδιαφέρει η προσάρτηση μόνο από εκείνο το VPS με το openSUSE. Γι' αυτό –αλλά και για λόγους ασφαλείας– με δύο μόλις κλικ απενεργοποιούμε το Samba support κι ενεργοποιούμε το WebDAV support. Αναφέραμε εξάλλου ότι στον u146187.your-storage.box υπάρχει ένας λογαριασμός μας, με username το u146187. Ποιο όμως είναι το αντίστοιχο password; Για να το μάθουμε, αρκεί ένα κλικ στο κουμπί Reset password (4). Εμφανίζεται τότε ένα pop-up και καλούμαστε να επιβεβαιώσουμε τη δημιουργία νέου password. Απαντάμε καταφατικά, με κλικ στο OK.



Μετά το Reset password το νέο συνθηματικό του χρήστη u146187 εμφανίζεται προσωρινά, στο πράσινο πλαίσιο πάνω πάνω. Πρέπει να το σημειώσουμε κάπου, αφού με το που θα φύγουμε από τη σελίδα το password δεν θα εμφανίζεται κάπου αλλού.

Προετοιμασία

Μετά την επιλογή και αγορά Storage Box από τη Hetzner, το βρίσκουμε από το μενού αριστερά επιλέγοντας Main functions / Storage boxes. Κάνουμε ένα κλικ πάνω στη γραμμή του –η ονομασία της γραμμής στην περίπτωση μας ήταν BX20 #135020– κι αμέσως αποκτάμε πρόσβαση σε όλες τις λεπτομέρειες που το αφορούν. Δείτε τα δύο screenshots που ακολουθούν, διαβάστε βεβαίως και τις αντίστοιχες περιγραφές.

Στο σημείο αυτό έχουμε ό,τι χρειαζόμαστε προκειμένου να προσαρτήσουμε το volume στο VPS μας, κατά το πρωτόκολλο WebDAV. Το θέμα είναι ότι το openSUSE δεν το γνωρίζει, οπότε κάτι πρέπει να κάνουμε και γι' αυτό.

Το WebDAV για το openSUSE

Πολύ γρήγορα διαπιστώσαμε ότι το λειτουργικό του VPS μας δεν υποστήριζε το πρωτόκολλο WebDAV. Αρχικά, ψάχνοντας στα repositories (αποθετήρια) της διανομής δεν βρήκαμε κάποιο σχετικό πακέτο. Κοιτάζοντας μετά και στο web, με χαρά διαπιστώσαμε ότι αρκεί να προσθέσουμε στο σύστημα ένα νέο repository, το οποίο μάλιστα υποστηρίζεται επίσημα από το project του openSUSE. Ευχάριστη η εξέλιξη, διότι διαφορετικά πρέπει να μπλέξουμε με μεταγλωττίσεις από το source. Χάρη σ' αυτό το repository, όμως, μπορούμε πολύ εύκολα να επαυξάνουμε τις ικανότητές της διανομής όσον αφορά στα filesystems. Η προσθήκη του εν λόγω αποθετηρίου γίνεται πληκτρολογώντας κάτι σαν αυτό:

```
sub0@vatnajokull:~> sudo zypper ar http://download.opensuse.org/repositories/
filesystems/openSUSE_Leap_42.2 'Leap422 Filesystems'
```

Αμέσως μετά ακολουθεί το φρεσκάρισμα των πληροφοριών για τα περιεχόμενα των αποθετηρίων:

```
cvar@vatnajokull:~> sudo zypper ref
```

Επειδή μόλις προσθέσαμε το νέο αποθετήριο για την υποστήριξη πρόσθετων filesystems, το zypper σταματά και μας ρωτά αν εμπιστευόμαστε το δημόσιο κλειδί του repository:

```
New repository or package signing key received:
  Repository:       Leap422 Filesystems
  Key Name:         filesystems OBS Project <filesystems@build.opensuse.org>
  Key Fingerprint:  B1FB5374 87204722 05FA6019 98C97FE7 324E6311
  Key Created:      þri 19.júl 2016, 16:36:42 CEST
  Key Expires:      fim 27.sep 2018, 16:36:42 CEST
  Rpm Name:         gpg-pubkey-324e6311-578e3afa
Do you want to reject the key, trust temporarily, or trust always? [r/t/a/?
shows all options] (r):
```

Μπορούμε να εμπιστευτούμε το κλειδί για την παρούσα λειτουργία της ανανέωσης, καθώς και για όλες όσες ακολουθήσουν: απλά πατάμε το πλήκτρο [A] (από το "Always") και δίνουμε ένα [Enter].

Μετά το φρεσκάρισμα, σειρά έχει η εγκατάσταση του πακέτου για την υποστήριξη του WebDAV:

```
sub0@vatnajokull:~> sudo zypper -n in davfs2
```

Τέλεια όλα.

Προσάρτηση του Storage Box

Πριν τη σύνδεση του volume στο τοπικό filesystem, φτιάχνουμε έναν βολικό κατάλογο κάτω από τον οποίο θα γίνει η προσάρτηση. Παράδειγμα:

```
sub0@vatnajokull:~> sudo mkdir /mnt/sbox
```

Είμαστε έτοιμοι για την προσάρτηση:

```
sub0@vatnajokull:~> sudo mount -t davfs https://u146187.your-storagebox.de /
mnt/sbox
```

Θα ερωτηθούμε για username και password. Το username είναι το hostname του μηχανήματος όπου βρίσκεται το volume (στο παράδειγμά μας u146187), ενώ το password είναι αυτό που εμφανίστηκε στο web panel της Hetzner και βεβαίως σημειώσαμε προσεκτικά. Αν όλα έχουν πάει καλά, στην έξοδο του εργαλείου df θα δούμε και μια γραμμή που αντιστοιχεί στο απομακρυσμένο volume:

```
sub0@vatnajokull:~> df -hT
Filesystem                        Type      Size  Used Avail Use% Mounted on
devtmpfs                          devtmpfs  979M     0  979M   0% /dev
tmpfs                             tmpfs    1000M     0 1000M   0% /dev/shm
tmpfs                             tmpfs    1000M  1.7M  999M   1% /run
tmpfs                             tmpfs    1000M     0 1000M   0% /sys/fs/cgroup
/dev/sda1                         ext4       47G  3.1G   42G   7% /
tmpfs                             tmpfs     200M     0  200M   0% /run/user/0
https://u146187.your-storagebox.de fuse      1.3T  763G  509G  61% /mnt/sbox
tmpfs                             tmpfs     200M     0  200M   0% /run/user/1000
```

Τα νούμερα που παρατίθενται στις στήλες Size και Used δεν έχουν σημασία, υπό την έννοια ότι δεν αντικατοπτρίζουν με ακρίβεια ούτε το μέγεθος του volume μας, επομένως ούτε και τον όγκο των δεδομένων που έχουμε αποθηκεύσει εκεί. Σημασία έχει μόνο το νούμερο στη στήλη Avail, το οποίο είναι ακριβές κι ανά πάσα στιγμή εκφράζει τον αποθηκευτικό χώρο που διαθέτουμε. Ας ρίξουμε και μια ματιά εντός του καταλόγου /mnt/sbox:

```
sub0@vatnajokull:~> ls -lh /mnt/sbox
total 0
drwx------ 2 root root 0 Feb 25 18:06 lost+found
```

Όπως βλέπετε, στο Storage Box προς το παρόν υπάρχει μόνον ο κατάλογος lost_found. Αυτός δημιουργήθηκε αυτόματα κατά τη διαμόρφωση του απομακρυσμένου filesystem. Θα προσέξατε ότι ανήκει στον χρήστη root, ενώ και η ομάδα του είναι εκείνη του root. Εμάς πάντως μας βολεύει περισσότερο όταν η προσάρτηση γίνεται από τον *απλό* χρήστη που έχουμε στο VPS μας. Για τη συγκεκριμένη διευθέτηση, αρχικά αποπροσαρτήσαμε το volume…

```
sub0@vatnajokull:~> sudo umount /mnt/sbox
```

…βρήκαμε το id του χρήστη μας και της ομάδας του…

```
sub0@vatnajokull:~> id sub0
uid=1000(sub0) gid=100(users) groups=100(users)
```

…και μετά προσαρτήσαμε ξανά ως εξής:

```
sub0@vatnajokull:~> sudo mount -t davfs -o uid=1000,gid=100 https://u146187.
your-storagebox.de /mnt/sbox
```

Η έξοδος του df απέδειξε ότι μετά την προσάρτηση την πλήρη δικαιοδοσία επί του volume την είχε ο χρήστης μας, όπως ακριβώς το θέλαμε:

```
sub0@vatnajokull:~> ls -lh /mnt/sbox
total 0
drwx------ 2 sub0 users 0 Feb 25 18:09 lost+found
```

Αυτοματισμός

Κάθε φορά που το VPS ενεργοποιείται ή επανεκκινεί, θέλουμε το Storage Box να προσαρτάται αυτόματα. Προς τούτο, με δικαιώματα διαχειριστή συστήματος αρκεί να προσθέσουμε στο αρχείο /etc/fstab μία γραμμή σαν την ακόλουθη:

```
https://u146187.your-storagebox.de /mnt/sbox davfs
noauto,rw,uid=1000,gid=100,file_mode=0660,dir_mode=0770 0 0
```

Με τη σημασία των παραμέτρων που έχουμε παραθέσει μετά το "davfs" δεν θα ασχοληθούμε τώρα, μπορείτε όμως να μάθετε περισσότερα πληκτρολογώντας

```
sub0@vatnajokull:~> man mount.davfs
```

(από το man βγαίνουμε πατώντας, απλά, το πλήκτρο [Q]). Θα πούμε μόνο για την επιλογή "noauto", η οποία εξαιρεί το filesystem από την εντολή mount -a που εκτελείται κατά την εκκίνηση του λειτουργικού και συνεπώς *δεν* προσαρτάται αυτόματα. Είναι βεβαίως λίγο αντιφατικό όλο αυτό, αφού *θέλουμε* να προσαρτάται αυτόματα. Το πρόβλημα είναι ότι η προσάρτηση επιχειρείται πριν ακόμα αρχικοποιηθεί το υποσύστημα δικτύωσης, επομένως αποτυγχάνει. Το μυστικό εδώ είναι ότι πρέπει να καθυστερήσουμε την προσάρτηση του απομακρυσμένου volume — ει δυνατόν να την αφήσουμε για το τέλος, όπου όλες οι υπηρεσίες του openSUSE θα έχουν ενεργοποιηθεί και ρυθμιστεί. Θα δούμε σε πολύ λίγο πώς ακριβώς πετυχαίνουμε αυτή την καθυστερημένη προσάρτηση. Προς το παρόν, να σημειώσουμε ότι στο τέλος του αρχείου /etc/davfs2/secrets πρέπει να βάλουμε μια γραμμή που θα μοιάζει με την ακόλουθη:

```
https://u146187.your-storagebox.de u146187 super_secret_password
```

Στο αρχείο /etc/davfs2/secrets έχει πρόσβαση ο χρήστης root και κανείς άλλος. Τα περιεχόμενά του διαβάζονται κάθε φορά που επιχειρείται προσάρτηση ενός WebDAV volume. Έτσι για τις προσαρτήσεις όπου απαιτούνται username και password τα αντίστοιχα στοιχεία βρίσκονται εντός του καλά προστατευμένου secrets κι όχι μέσα στο

fstab, το οποίο μπορούν να διαβάζουν ακόμη και οι απλοί χρήστες του συστήματος. Ας δούμε τώρα πώς μετά το τέλος της εκκίνησης του λειτουργικού θα προσαρτάται αυτόματα το Storage Box μας. Υπάρχουν βεβαίως περισσότεροι του ενός τρόποι για να συμβαίνει αυτό, ο ευκολότερος όμως ίσως είναι με ένα νέο cronjob. Αναλυτικότερα, πληκτρολογούμε

```
sub0@vatnajokull:~> sudo crontab -e
```

και στο τέλος του αρχείου crontab προσθέτουμε μια γραμμή σαν την ακόλουθη:

```
@reboot /usr/bin/mount /mnt/sbox
```

Αποθηκεύουμε την αλλαγή και για δοκιμή επανεκκινούμε το VPS μας. Αν όλα έχουν πάει καλά –που δεν βλέπουμε το λόγο για να μην έχουν πάει, δηλαδή– τότε το Storage Volume θα είναι προσαρτημένο και πλήρως προσβάσιμο από τον χρήστη μας.

Από τις πολλές εφαρμογές που βρίσκει το Storage Box, μία που μπορούμε να σκεφτούμε είναι ν' αποτελέσει το χώρο αποθήκευσης για ένα Nextcloud instance στο cloud. Όπως και να το κάνουμε, το data directory του Nextcloud δεν είναι απαραίτητο να κατοικεί στην ίδια κατάτμηση που κατοικεί κι ο web server.



Στις επιλογές που υπάρχουν στη γραμμή του fstab για την προσάρτηση του απομακρυσμένου Storage Box μέσω WebDAV (1), υπάρχει και η noauto: επειδή η προσάρτηση θα επιχειρηθεί πριν ακόμα αρχικοποιηθεί το υποσύστημα δικτύωσης, η διαδικασία θα αποτύχει. Καθυστερούμε, λοιπόν, την προσάρτηση και την πραγματοποιούμε μέσω κατάλληλου cronjob (βλ. "@reboot") αμέσως μετά την ολοκλήρωση του boot. Παρεμπιπτόντως, στο αρχείο /etc/davfs2/secrets πρέπει να υπάρχει μια γραμμή με το URL του server που φιλοξενεί το Storage Volume, το username μας εκεί καθώς και το αντίστοιχο password (2). Σημειώστε ότι πρόσβαση στο secrets έχει μόνον ο χρήστης root, ενώ στο fstab έχουν δικαιώματα ανάγνωσης ακόμα και οι απλοί χρήστες.

Skill: Intermediate
Tags: kernel, openSUSE

Πώς θα έχετε πάντα το νεότερο πυρήνα στο openSUSE Leap

Η έκδοση του Linux kernel στο openSUSE Leap 42.2 είναι η 4.4 και φυσικά υποστηρίζεται επίσημα από το openSUSE project. Αυτό σημαίνει ότι ανανεώνεται κάθε φορά που εντοπίζεται κάποιο bug ή πρόβλημα ασφαλείας. Η βασική έκδοση του πυρήνα, ωστόσο, δεν αλλάζει.

Συγκεκριμένα, τη στιγμή που γράφονται αυτές οι γραμμές στο Leap 42.2 έχουμε τον πυρήνα 4.4.49-16.1. Με μια βόλτα στο δικτυακό τόπο kernel.org, όπου δημοσιεύονται διαρκώς οι νέες εκδόσεις του πυρήνα, βλέπουμε ότι η πλέον πρόσφατη έκδοση είναι η 4.10.1. Πώς άραγε αναβαθμίζουμε το openSUSE μας ώστε να βασίζεται στο νεότερο πυρήνα;

Ένας τρόπος είναι να κατεβάσουμε το source code του kernel, να τον μεταγλωττίσουμε και μετά να τον εγκαταστήσουμε. Το πώς ακριβώς εργαζόμαστε σε μια τέτοια περίπτωση μπορείτε να δείτε σε σχετικό βίντεο που έχουμε ετοιμάσει (https://deltahacker.gr/?p=16567). Εναλλακτικά μπορούμε να προσθέσουμε στο λειτουργικό ένα νέο repository (αποθετήριο) από το openSUSE project, το οποίο περιλαμβάνει πακέτα RPM με τις νεότερες εκδόσεις του πυρήνα. Κατ' αυτόν τον τρόπο παρακάμπτουμε το εξαιρετικά χρονοβόρο στάδιο της μεταγλώττισης από το source code, ενώ παίρνουμε κι έναν πυρήνα με patches ειδικά για το openSUSE.

Για την προσθήκη του νέου αποθετηρίου γράφουμε:

```
cvar@holmavik:~> sudo zypper ar -f \
> http://download.opensuse.org/repositories/Kernel:/HEAD/standard \
> 'Leap422 Kernel'
Adding repository 'Leap422 Kernel' .....................[done]
Repository 'Leap422 Kernel' successfully added

URI          : http://download.opensuse.org/repositories/Kernel:/HEAD/standard
Enabled      : Yes
GPG Check    : Yes
```

```
Autorefresh : Yes
Priority    : 99 (default priority)

Repository priorities are without effect. All enabled repositories share the
same priority.
```

Όλα τα repositories του λειτουργικού, συμπεριλαμβανομένου κι εκείνου που μόλις προσθέσαμε, τα βλέπουμε πληκτρολογώντας:

```
cvar@holmavik:~> zypper lr
Repository priorities are without effect. All enabled repositories share the same priority.

# | Alias                             | Name                                  | Enabled | GPG Check |
Refresh
--+-----------------------------------+---------------------------------------+---------+-----------+----
1 | Leap422 Kernel                    | Leap422 Kernel                        | Yes     | ( p) Yes  | Yes
2 | download.opensuse.org-filesystems | Leap422 Filesystems                   | Yes     | (r ) Yes  | Yes
3 | download.opensuse.org-non-oss     | Leap422 Main Repository Non-OSS       | Yes     | (r ) Yes  | Yes
4 | download.opensuse.org-non-oss_1   | Leap422 Main Repository Non-OSS Updates | Yes   | (r ) Yes  | Yes
5 | download.opensuse.org-oss         | Leap422 Main Repository OSS           | Yes     | (r ) Yes  | Yes
6 | download.opensuse.org-oss_1       | Leap422 Main Repository OSS Updates   | Yes     | (r ) Yes  | Yes
7 | opensuse-guide.org-repo           | Leap422 LibDVDCSS                     | Yes     | (r ) Yes  | Yes
8 | packman.inode.at-suse             | Leap422 Packman                       | Yes     | (r ) Yes  | Yes
```

Στη συνέχεια φρεσκάρουμε τα περιεχόμενα των repositories του openSUSE μας:

```
cvar@holmavik:~> sudo zypper ref
Repository 'Leap422 Filesystems' is up to date.
Retrieving repository 'Leap422 Kernel' metadata ............[done]
Building repository 'Leap422 Kernel' cache .................[done]
Repository 'Leap422 Main Repository Non-OSS' is up to date.
Repository 'Leap422 Main Repository Non-OSS Updates' is up to date.
Repository 'Leap422 Main Repository OSS' is up to date.
Repository 'Leap422 Main Repository OSS Updates' is up to date.
Repository 'Leap422 LibDVDCSS' is up to date.
Repository 'Leap422 Packman' is up to date.
All repositories have been refreshed.
```

Προκειμένου ν' αναβαθμίσουμε το λειτουργικό σύστημα χρησιμοποιώντας το νέο kernel repository, δίνουμε:

```
cvar@holmavik:~> sudo zypper dup --repo='Leap422 Kernel'
```

Σημείωση. Για τις αναβαθμίσεις από συγκεκριμένο repository καλό είναι να αποφεύγουμε την παράμετρο --repo και στη θέση της να χρησιμοποιούμε τη --from. Σε αντίθεση με τη --repo, η παράμετρος --from *δεν* κρύβει από τον resolver τα ενεργοποιημένα αποθετήρια της εγκατάστασής μας που *δεν* αναφέρονται στην εντολή αναβάθμισης. Έτσι, σε περίπτωση που χρειάζεται να ικανοποιηθούν dependencies (εξαρτήσεις) λαμβάνονται *όλα* τα απαραίτητα αποθετήρια υπόψη.

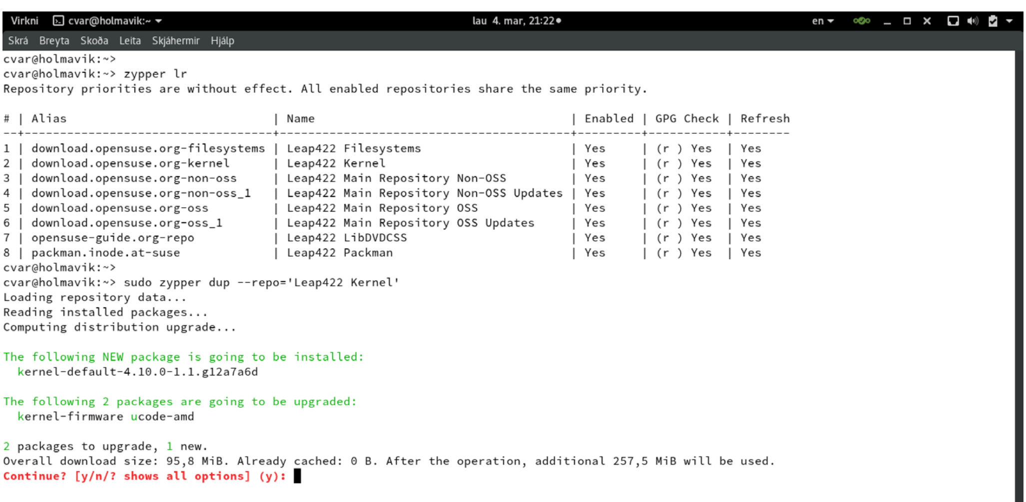
Μετά τη διαδικασία της αναβάθμισης οφείλουμε να επανεκκινήσουμε το σύστημα:

```
cvar@holmavik:~> sudo reboot
```

Αφού το reboot ολοκληρωθεί, ένας τρόπος για να επαληθεύσουμε ότι πράγματι έχουμε τη νέα έκδοση του πυρήνα είναι να γράψουμε:

```
cvar@holmavik:~> uname -a
Linux holmavik.colder.xyz 4.10.0-1.g12a7a6d-default #1 SMP PREEMPT
Mon Feb 20 13:08:30 UTC 2017 (12a7a6d) x86_64 x86_64 x86_64 GNU/Linux
```

Χαρείτε το νέο σας Leap!



Το νέο repository με τις πρόσφατες εκδόσεις του Linux kernel (1) έχει ήδη προστεθεί στο openSUSE μας, και τώρα είμαστε έτοιμοι ν' αναβαθμίσουμε το λειτουργικό σύστημα (2) ώστε να τρέχουμε την πιο νέα έκδοση του πυρήνα.


CMYK & WEB
cmykandweb.gr
GRAPHIC DESIGN
design • layout • web

Skill: Intermediate
Tags: LEMP, openSUSE, nginx, MariaDB, PHP, server blocks

Χτίσιμο LEMP stack στο openSUSE

Το ακρωνύμιο LEMP αναφέρεται στο σύνολο του λογισμικού που αποτελείται από τον διακομιστή ιστοσελίδων nginx (προφέρεται engine-ex), τη σχεσιακή βάση δεδομένων MySQL, τη σκριπτογλώσσα PHP και κάποια διανομή του Linux. Ένα μηχάνημα με LEMP stack, όπως λέμε, είναι ικανό να σερβίρει web sites με δυναμικό περιεχόμενο ή να φιλοξενεί web applications γενικότερα.

Αν για παράδειγμα θέλετε να βασίσετε το site σας στο WordPress, τότε μία από τις επιλογές σας είναι ένας server με LEMP stack. Στο παρόν άρθρο δείχνουμε, αναλυτικά και βήμα προς βήμα, πώς εγκαθιστούμε μια τέτοια στοίβα λογισμικού όταν έχουμε έναν host με openSUSE Leap και αντί για τη MySQL θέλουμε να χρησιμοποιήσουμε τη MariaDB. Για την εφαρμογή των ενεργειών που περιγράφουμε μπορείτε να εργαστείτε σε ένα VPS με openSUSE –οι Hetzner και Linode είναι δύο VPS providers που υποστηρίζουν *και* το openSUSE– ή, εναλλακτικά, σε μια εικονική μηχανή ή σ' έναν τοπικό server.

VPS με openSUSE Leap

Στο https://deltahacker.gr/?p=16962 φιλοξενούμε άρθρο για την εγκατάσταση και τη ρύθμιση του openSUSE Leap σε VPS της Hetzner. Όλα όσα παρουσιάζουμε και συζητάμε για το openSUSE εφαρμόζονται παρόμοια κι όταν έχετε άλλον provider ή όταν δουλεύετε σε εικονική μηχανή ή τοπικό server.

Προετοιμασία συστήματος κι εγκατάσταση nginx

Μέσω SSH συνδεόμαστε στον host με το openSUSE κι αποκτάμε πρόσβαση στο λογαριασμό του root. Έχουμε βεβαίως τη δυνατότητα να εργαστούμε κι από το λογαριασμό κάποιου απλού χρήστη, αρκεί αυτός να έχει τη δυνατότητα ανάληψης δικαιωμάτων root, π.χ., μέσω του εργαλείου sudo.

Πρώτο μας μέλημα είναι να φρεσκάρουμε τα περιεχόμενα των αποθετηρίων (repositories):

```
hekla:~ # zypper ref
```

Μετά εφαρμόζουμε patches, αν υπάρχουν, με ενημερώσεις ασφαλείας και bug fixes:

```
hekla:~ # zypper patch
```

Ξεκινάμε με το πρώτο συστατικό του LEMP stack, το οποίο δεν είναι άλλο από τον nginx:

```
hekla:~ # zypper -n in nginx
```

Μετά την εγκατάστασή του στο openSUSE, ο nginx δεν τρέχει:

```
hekla:~ # systemctl status nginx
● nginx.service - The nginx HTTP and reverse proxy server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; disabled; vendor
preset: disabled)
   Active: inactive (dead)
```

Τον ξεκινάμε, λοιπόν...

```
hekla:~ # systemctl start nginx
```

...φροντίζουμε ώστε η αντίστοιχη υπηρεσία να ενεργοποιείται αυτόματα κατά την εκκίνηση του λειτουργικού...

```
hekla:~ # systemctl enable nginx
Created symlink from /etc/systemd/system/multi-user.target.wants/nginx.service
to /usr/lib/systemd/system/nginx.service.
```

...και βεβαιωνόμαστε ότι όλα είναι καλά:

```
hekla:~ # systemctl status -l nginx
● nginx.service - The nginx HTTP and reverse proxy server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; vendor
preset: disabled)
   Active: active (running) since fös 2017-04-14 06:59:56 GMT; 2min 38s ago
 Main PID: 3921 (nginx)
   CGroup: /system.slice/nginx.service
           ├─3921 nginx: master process /usr/sbin/nginx -g daemon off
           └─3925 nginx: worker process
```

Για το Systemd και τη διαχείριση υπηρεσιών, όπως είναι εκείνη του nginx, μπορείτε να διαβάσετε το σχετικό άρθρο που φιλοξενούμε στο https://deltahacker.gr/?p=16816.

Πιθανώς το firewall να είναι ενεργοποιημένο για τον server μας –ή τουλάχιστον έτσι θα έπρεπε–, οπότε σ' αυτή την περίπτωση οφείλουμε να βεβαιωθούμε ότι το port 80/TCP είναι ανοικτό. Υποθέτουμε ότι το firewall είναι πράγματι ενεργοποιημένο, καθώς κι ότι αρχικά επιτρέπει την πρόσβαση μόνο στο port 22/TCP (για συνδέσεις SSH). Παρεμπιπτόντως, να ένας τρόπος για να βλέπουμε την κατάστασή του:

```
hekla:~ # systemctl status SuSEfirewall2
● SuSEfirewall2.service - SuSEfirewall2 phase 2
   Loaded: loaded (/usr/lib/systemd/system/SuSEfirewall2.service; enabled;
vendor preset: disabled)
   Active: active (exited) since fös 2017-04-14 06:45:59 GMT; 39min ago
 Main PID: 3591 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/SuSEfirewall2.service
```

Πώς του ζητάμε να επιτρέπει και συνδέσεις στο port 80/TCP; Υπάρχουν διάφοροι τρόποι κι αμέσως τώρα ακολουθούμε έναν ο οποίος θα μπορούσε να λεχθεί ότι είναι συμβατός με το "openSUSE way". Αρχικά, μεταβαίνουμε στον κατάλογο /etc/sysconfig/SuSEfirewall2.d/services:

```
hekla:~ # cd /etc/sysconfig/SuSEfirewall2.d/services
```

Ρίξτε μια ματιά στα περιεχόμενά του:

```
hekla:/etc/sysconfig/SuSEfirewall2.d/services # ls -lh
total 32K
-rw-r--r-- 1 root root  146 júl 22  2016 mosh
-rw-r--r-- 1 root root  707 apr  5 12:11 nfs-client
-rw-r--r-- 1 root root  343 des 19 17:18 ntp
-rw-r--r-- 1 root root  762 okt  8  2016 rsync-server
-rw-r--r-- 1 root root  126 mar 29 14:35 samba-client
-rw-r--r-- 1 root root  375 okt  8  2016 smtp
-rw-r--r-- 1 root root  135 jan 25 08:51 sshd
-rw-r--r-- 1 root root 1,5K okt  7  2016 TEMPLATE
```

Διάφορες υπηρεσίες αφήνουν εδώ αρχεία ρυθμίσεων για το SuSEfirewall2. Στα εν λόγω αρχεία κατ' ελάχιστον παρατίθενται τα ports που πρέπει να είναι ανοικτά για το External Zone του firewall. Το πακέτο nginx που μόλις εγκαταστήσαμε δεν έχει αφήσει κάποιο σχετικό αρχείο στον κατάλογο services. Γι' αυτό κι εμείς θ' αντιγράψουμε το TEMPLATE, μετονομάζοντάς το σε nginx:

```
hekla:/etc/sysconfig/SuSEfirewall2.d/services # cp TEMPLATE nginx
```

Το τροποποιούμε καταλλήλως με τον text editor της προτίμησής μας:

```
hekla:/etc/sysconfig/SuSEfirewall2.d/services # vi nginx
```

Δείτε τα περιεχόμενα του δικού μας nginx:

```
## Name: nginx
## Description: Open ports 80/TCP & 443/TCP for the nginx web server
# space separated list of allowed TCP ports
TCP="80 443"
```

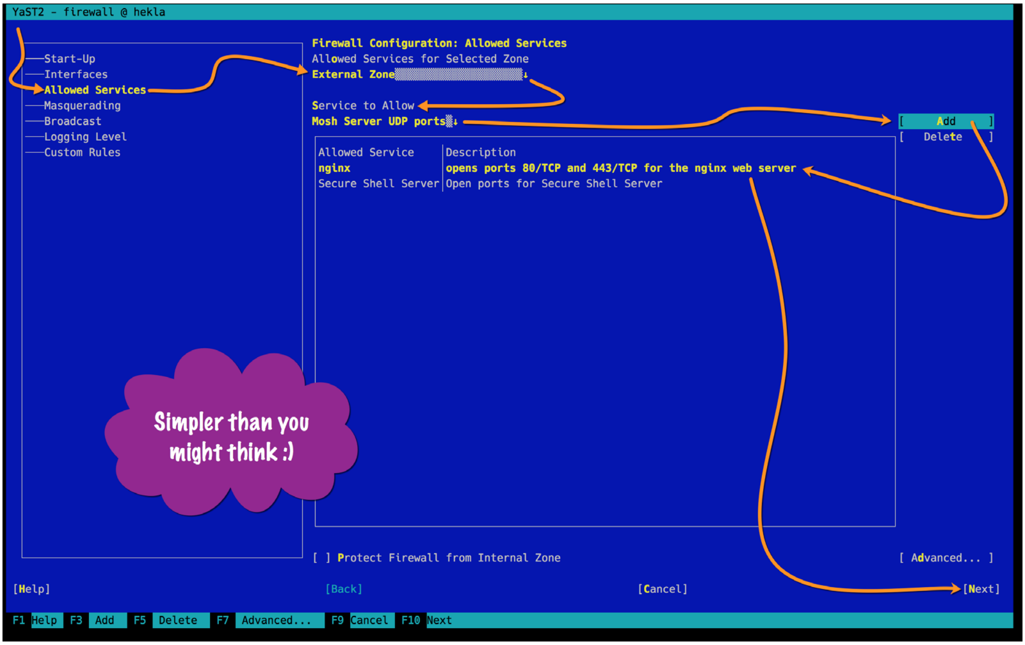
Αν και πριν λίγο σκεφτήκαμε ν' ανοίξουμε το port 80/TCP για απλές συνδέσεις HTTP, ανοίξαμε τελικά και το port 443/TCP για ασφαλείς συνδέσεις HTTPS. Είτε φτιάξουμε το δικό μας self-signed πιστοποιητικό είτε πάρουμε ένα έγκυρο από το Let's Encrypt project, με μηδενικό κόστος θα παρέχουμε ασφαλείς συνδέσεις TLS για τα sites και τις εφαρμογές που φιλοξενεί ο nginx. Αλλά για το όλο θέμα θα συζητήσουμε σε άλλο άρθρο, με την άνεσή μας. Προς το παρόν, ας υποδείξουμε στο firewall τα δύο νέα ports τα οποία πρέπει να είναι ανοικτά. Καταφεύγουμε στο module του YaST ονόματι firewall:

```
hekla:/etc/sysconfig/SuSEfirewall2.d/services # yast firewall
```

Στο screenshot που ακολουθεί φαίνεται το πώς ανοίξαμε τα δύο ports του nginx για το External Zone του firewall.

Αφού εγκαταλείψουμε το YaST, ας βεβαιωθούμε ότι τα ports 80/TCP και 443/TCP είναι ανοικτά:

```
hekla:~ # iptables -S
[...]
-A input_ext -p tcp -m limit --limit 3/min -m tcp --dport 80 --tcp-flags
FIN,SYN,RST,ACK SYN -j LOG --log-prefix "SFW2-INext-ACC-TCP " --log-tcp-options
--log-ip-options
```



Χάρη στο module του YaST ονόματι firewall, είναι πολύ εύκολο να επιτρέψουμε την πρόσβαση από τον έξω κόσμο στα δύο ports που χρησιμοποιεί ο nginx web server.

```
-A input_ext -p tcp -m tcp --dport 80 -j ACCEPT
-A input_ext -p tcp -m limit --limit 3/min -m tcp --dport 443 --tcp-flags
FIN,SYN,RST,ACK SYN -j LOG --log-prefix "SFW2-INext-ACC-TCP " --log-tcp-options
--log-ip-options
-A input_ext -p tcp -m tcp --dport 443 -j ACCEPT
[...]
```

Μια χαρά όλα, μόνο που ξεχάσαμε να δούμε τι γίνεται με τον nginx. Μεταβαίνουμε αμέσως στον κατάλογο /srv/www/htdocs και φτιάχνουμε ένα πολύ απλό αρχείο HTML, το οποίο περιλαμβάνει ένα σύντομο μήνυμα καλωσορίσματος (σε όποια γλώσσα θέλουμε :D):

```
hekla:/srv/www/htdocs # echo "<h1>Velkomið að nginx @ hekla.colder.local</h1>"
> index.html
```

(Το hekla.colder.local είναι το FQDN του host με το openSUSE, για το τοπικό μας δίκτυο.) Ανοίγουμε έναν οποιονδήποτε web browser και στη μπάρα διευθύνσεων γράφουμε το FQDN ή το αριθμητικό IP του host με το openSUSE. Αν δούμε το μήνυμα καλωσορίσματος που μόλις πληκτρολογήσαμε, τότε ο nginx είναι πολύ χαρούμενος και δουλεύει μια χαρά.



Βρείτε το *πραγματικά* δημόσιο IP

Αν διαθέτουμε κάποιο domain και, για αυτό ή για κάποιο subdomain του σχεδιάζουμε να δημιουργήσουμε ένα A record που θα δείχνει προς τον host με το openSUSE, χρειαζόμαστε το δημόσιο IP του προαναφερθέντος. Προσέξτε ότι αυτό δεν είναι κατ' ανάγκη εκείνο που παρατίθεται στην έξοδο της εντολής `ip addr`, ακόμη κι αν εργαζόμαστε σε VPS (ορισμένοι providers, όπως η Hetzner, έχουν τα VPS των πελατών πίσω από NAT firewalls). Ένας τρόπος για να μαθαίνουμε το δημόσιο IP με το οποίο ο server μας φαίνεται στο Internet, είναι πληκτρολογώντας `dig +short myip.opendns.com @resolver1.opendns.com`.

Εγκατάσταση και ρύθμιση MariaDB

Η εγκατάσταση της MariaDB γίνεται κατά τα αναμενόμενα:

```
hekla:~ # zypper -n in mariadb
```

Με την ολοκλήρωση της διαδικασίας συνειδητοποιούμε ότι υπήρχε κάποιο ενημερωτικό μήνυμα, το οποίο όμως δεν εμφανίστηκε λόγω της χρήσης της παραμέτρου -n:

```
Update notifications were received from the following packages:
mariadb-10.0.29-18.1.x86_64 (/var/adm/update-messages/mariadb-10.0.29-18.1)
View the notifications now? [y/n] (n): n
```

Το μήνυμα που δεν είδαμε είναι στο αρχείο /var/adm/update-messages/mariadb-10.0.29-18.1, οπότε ας του ρίξουμε μια ματιά τώρα:

```
hekla:~ # cat /var/adm/update-messages/mariadb-10.0.29-18.1
You just installed MySQL server for the first time.

You can start it using:
 rcmysql start

During first start empty database will be created for your automatically.

PLEASE REMEMBER TO SET A PASSWORD FOR THE MariaDB root USER !
To do so, start the server, then issue the following commands:

'/usr/bin/mysqladmin' -u root password 'new-password'
'/usr/bin/mysqladmin' -u root -h <hostname> password 'new-password'

Alternatively you can run:
'/usr/bin/mysql_secure_installation'

which will also give you the option of removing the test
databases and anonymous user created by default. This is
strongly recommended for production servers.
```

Μάλιστα. Η σημαντική πληροφορία στο προηγούμενο μήνυμα είναι ότι, προκειμένου να έχουμε μια ασφαλή εγκατάσταση της MariaDB, οφείλουμε να τρέξουμε το script ονόματι /usr/bin/mysql_secure_installation. Πρώτα ενεργοποιούμε την υπηρεσία της MariaDB...

```
hekla:~ # systemctl start mysql
```

...μετά βεβαιωνόμαστε ότι τρέχει...

```
hekla:~ # systemctl status mysql
● mysql.service - MySQL server
   Loaded: loaded (/usr/lib/systemd/system/mysql.service; disabled; vendor
preset: disabled)
   Active: active (running) since fös 2017-04-14 09:41:40 GMT; 53s ago
```

```
  Process: 2601 ExecStartPost=/usr/lib/mysql/mysql-systemd-helper wait
(code=exited, status=0/SUCCESS)
  Process: 2587 ExecStartPre=/usr/lib/mysql/mysql-systemd-helper upgrade
(code=exited, status=0/SUCCESS)
  Process: 2493 ExecStartPre=/usr/lib/mysql/mysql-systemd-helper install
(code=exited, status=0/SUCCESS)
 Main PID: 2600 (mysqld)
    Tasks: 23 (limit: 512)
   CGroup: /system.slice/mysql.service
           └─2600 /usr/sbin/mysqld --defaults-file=/etc/my.cnf --user=mysql
```

...ύστερα τρέχουμε το /usr/bin/mysql_secure_installation:

```
hekla:~ # /usr/bin/mysql_secure_installation
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user.  If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

Set root password? [Y/n] Y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
 ... Success!

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
```

```
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] Y
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] Y
 ... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] Y
 - Dropping test database...
 ... Success!
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.
Reload privilege tables now? [Y/n] Y
 ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

Εξ ορισμού, το password για τον χρήστη root της MariaDB δεν υπάρχει, γι' αυτό κι όταν μας ζητείται πατάμε απλά το πλήκτρο [Enter]. Στη συνέχεια ορίζουμε ένα password για το χρήστη root της MariaDB (για λόγους ασφαλείας το πληκτρολογούμε δύο φορές και δεν φαίνεται στο τερματικό), διαγράφουμε τους υπάρχοντες ανώνυμους χρήστες της βάσης, απαγορεύουμε τα απομακρυσμένα login στο λογαριασμό root

της MariaDB, διαγράφουμε την υπάρχουσα δοκιμαστική βάση και, τέλος, υποχρεώνουμε το σύστημα να λάβει υπόψη όλες τις αλλαγές που μόλις πραγματοποιήσαμε. Όπως διαπιστώνετε κι εσείς, εκτός από τον καθορισμό password για τον root της MariaDB σε *όλες* τις άλλες ερωτήσεις αρκεί να δώσουμε τις προεπιλεγμένες απαντήσεις.

Θέλουμε η MariaDB να ξεκινά αυτόματα κατά την εκκίνηση του λειτουργικού, γι' αυτό κι ενεργοποιούμε τη σχετική υπηρεσία:

```
hekla:~ # systemctl enable mysql
Created symlink from /etc/systemd/system/multi-user.target.wants/mysql.service
to /usr/lib/systemd/system/mysql.service.
```

Γιατί βλέπουμε διαρκώς αναφορές στη MySQL;

Η MariaDB αναπτύσσεται από την κοινότητα του Ανοικτού/Ελεύθερου Λογισμικού και αποτελεί fork της γνωστής MySQL, η οποία από το 2010 ανήκει στην Oracle. Οι συχνές εμφανίσεις του ονόματος MySQL δεν πρέπει να μας προκαλούν εντύπωση, αφού η MariaDB έχει σχεδιαστεί ως drop-in replacement της MySQL. Μ' άλλα λόγια, όποιο εργαλείο ή εντολή χρησιμοποιούμε σε μια εγκατάσταση της MySQL, το ίδιο ακριβώς εργαλείο ή εντολή χρησιμοποιούμε και σε μια εγκατάσταση της MariaDB.

Εγκατάσταση PHP για την παραγωγή δυναμικού περιεχομένου

Στο LEMP stack που χτίζουμε προς το παρόν υπάρχει το Linux (προφανώς), ο web server (nginx), καθώς και η σχεσιακή βάση δεδομένων (MariaDB). Ο nginx σερβίρει ιστοσελίδες, ενώ η MariaDB αποθηκεύει δεδομένα και συσχετισμούς μεταξύ διαφορετικών οντοτήτων. Αυτό που λείπει είναι κάτι για την παραγωγή δυναμικού περιεχομένου. Θα καταφύγουμε στη γλώσσα PHP. Επειδή ο nginx δεν έχει την παραμικρή ιδέα για την PHP, θα εγκαταστήσουμε πρώτα το module από το πακέτο php5-fpm (FastCGI Process Manager) και, μετά από ορισμένες απαραίτητες ρυθμίσεις, θα πούμε στον web server να στέλνει τα όποια αιτήματα PHP στην αντίστοιχη διεργασία. Θα εγκαταστήσουμε επίσης και το module από το πακέτο php5-mysql, ώστε η PHP να είναι σε θέση να επικοινωνεί με τη MariaDB. Υπάρχει και μια σειρά από άλλα πακέτα που αξίζει να εγκαταστήσουμε, τα οποία για τις ανάγκες του παρόντος δεν έχει νόημα ν' αναφέρουμε ένα προς ένα:

```
hekla:~ # zypper -n in php5 php5-gd php5-fpm php5-pear php5-mysql php5-gettext
php5-suhosin php5-mbstring
```

Μετά την εγκατάσταση των πακέτων πηγαίνουμε στον κατάλογο /etc/php5/fpm...

```
hekla:~ # cd /etc/php5/fpm
```

...και αντιγράφουμε το αρχείο php-fpm.conf.default στο php-fpm.conf:

```
hekla:/etc/php5/fpm # cp php-fpm.conf.default php-fpm.conf
```

Ανοίγουμε το αρχείο php-fpm.conf με τον editor της προτίμησής μας και φροντίζουμε ώστε οι γραμμές...

```
;error_log = log/php-fpm.log
user = nobody
group = nobody
listen = 127.0.0.1:9000
;listen.owner = nobody
;listen.group = nobody
;listen.mode = 0660
```

...να τροποποιηθούν και να γίνουν όπως οι ακόλουθες:

```
error_log = log/php5-fpm.log
user = nginx
group = nginx
listen = /var/run/php5-fpm.sock
listen.owner = nginx
listen.group = nginx
listen.mode = 0660
```

Αν βοηθάει, ιδού και το diff μεταξύ του πρωτότυπου αρχείου php-fpm.conf.default και του τροποποιημένου php-fpm.conf:

```
hekla:/etc/php5/fpm # diff php-fpm.conf.default php-fpm.conf
32c32
< ;error_log = log/php-fpm.log
---
> error_log = log/php5-fpm.log
148,149c148,149
< user = nobody
```

```
< group = nobody
---
> user = nginx
> group = nginx
159c159
< listen = 127.0.0.1:9000
---
> listen = /var/run/php5-fpm.sock
170,172c170,172
< ;listen.owner = nobody
< ;listen.group = nobody
< ;listen.mode = 0660
---
> listen.owner = nginx
> listen.group = nginx
> listen.mode = 0660
```

Αφού τελειώσουμε με τις αλλαγές στο php-fpm.conf πηγαίνουμε στον κατάλογο /etc/php5/cli:

```
hekla:/etc/php5/fpm # cd /etc/php5/cli
```

Ανοίγουμε το αρχείο php.ini, εντοπίζουμε τη γραμμή

```
;cgi.fix_pathinfo=1
```

και την αλλάζουμε ώστε να είναι ακριβώς όπως η ακόλουθη:

```
cgi.fix_pathinfo=0
```

Χωρίς αυτή την αλλαγή, όποτε ζητείται ένα αρχείο που δεν υπάρχει τότε η PHP προσπαθεί να εκτελέσει το πιο "κοντινό" αρχείο που μπορεί να εντοπίσει. Έτσι, ένας επιτιθέμενος είναι εύκολο να προκαλέσει την εκτέλεση αρχείων στα οποία κανονικά δεν θα έπρεπε να έχει πρόσβαση. Αποθηκεύουμε την αλλαγή μας στο php.ini και το αντιγράφουμε στον κατάλογο /etc/php5/conf.d:

```
hekla:/etc/php5/cli # cp php.ini ../conf.d
```

Στο σημείο αυτό έχουμε τελειώσει με τη ρύθμιση της PHP, μένει όμως να πείσουμε και τον nginx να συνεργαστεί με τον processor της γλώσσας (εν προκειμένω με το php5-fpm).

Συνεργασία nginx και PHP

Η συνεργασία επιτυγχάνεται σε επίπεδο server block, δηλαδή ανά site που φιλοξενεί και σερβίρει ο nginx. Τα server blocks του nginx είναι αντίστοιχα των virtual hosts του Apache (https://deltahacker.gr/?p=17194) και το προκαθορισμένο server block περιγράφεται στο αρχείο /etc/nginx/nginx.conf. Το ανοίγουμε με κάποιον text editor και πραγματοποιούμε τις ακόλουθες δύο αλλαγές.

1. Στο τμήμα

```
location / {
root    /srv/www/htdocs/;
index   index.html index.htm;
}
```

και συγκεκριμένα στη γραμμή

```
index   index.html index.htm;
```

προσθέτουμε ένα index.php ώστε να γίνει έτσι:

```
index   index.php index.html index.htm;
```

2. Κάτω από το τμήμα

```
error_page   500 502 503 504  /50x.html;
location = /50x.html {
root    /srv/www/htdocs/;
}
```

προσθέτουμε το ακόλουθο τμήμα:

```
location ~ \.php$ {
root /srv/www/htdocs;
```

```
try_files $uri =404;
include /etc/nginx/fastcgi_params;
fastcgi_pass unix:/var/run/php5-fpm.sock;
fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
}
```

Αποθηκεύουμε τις αλλαγές στο nginx.conf κι ελέγχουμε το συντακτικό του αρχείου για λάθη:

```
hekla:/etc/nginx # nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

Εν συνεχεία ξεκινάμε την υπηρεσία php-fpm (χωρίς το "5")...

```
hekla:/etc/nginx # systemctl status php-fpm.service
```

...και φροντίζουμε ώστε να ενεργοποιείται αυτόματα κατά την εκκίνηση του openSUSE:

```
hekla:/etc/nginx # systemctl enable php-fpm.service
Synchronizing state of php-fpm.service with SysV init with /usr/lib/systemd/
systemd-sysv-install...
Executing /usr/lib/systemd/systemd-sysv-install enable php-fpm
Warning: //etc/init.d/php-fpm is masked by /usr/lib/systemd/system/php-fpm.
service.
Try 'chkconfig php-fpm on' instead
Created symlink from /etc/systemd/system/multi-user.target.wants/php-fpm.
service to /usr/lib/systemd/system/php-fpm.service.
```

Βεβαίως, επανεκκινούμε και τον nginx:

```
hekla:/etc/nginx # systemctl restart nginx
```

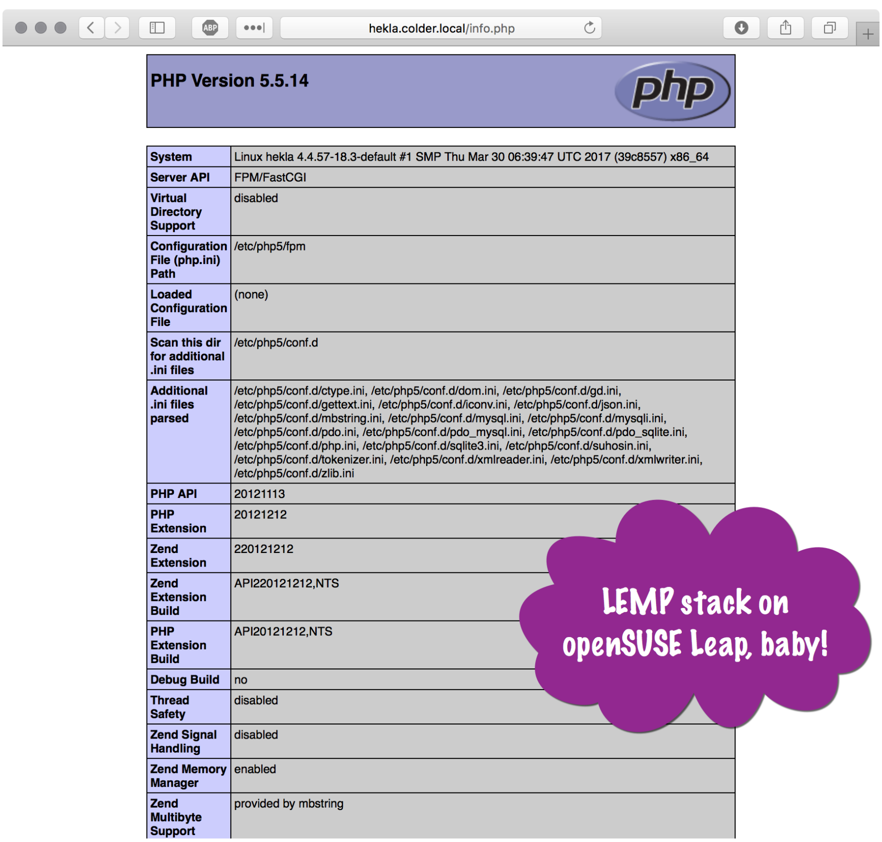
Πώς βεβαιωνόμαστε ότι ο nginx πράγματι συνεργάζεται με την PHP; Πολύ καλό ερώτημα. Πηγαίνουμε στον κατάλογο που χρησιμοποιεί το προκαθορισμένο server block, ο οποίος δεν είναι άλλος από τον /srv/www/htdocs:

```
hekla:/etc/nginx # cd /srv/www/htdocs
```

Δημιουργούμε εκεί ένα πολύ απλό αρχείο PHP, το οποίο όταν εκτελείται επιστρέφει πληροφορίες για το σύστημα:

```
hekla:/srv/www/htdocs # echo "<?php phpinfo(); ?>" > info.php
```

Από έναν web browser πηγαίνουμε στη διεύθυνση http://hekla.colder.local/info.php, όπου βέβαια στη θέση του hekla.colder.local εσείς θα βάλετε είτε το FQDN είτε το αριθμητικό IP του δικού σας server. Αν όλα έχουν πάει καλά, στον browser θα δούμε πληθώρα πληροφοριών για το σύστημα. Και κάπως έτσι, λοιπόν, αποκτήσαμε έναν openSUSE Leap server με καλορυθμισμένο LEMP stack.



System	Linux hekla 4.4.57-18.3-default #1 SMP Thu Mar 30 06:39:47 UTC 2017 (39c8557) x86_64
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/fpm
Loaded Configuration File	(none)
Scan this dir for additional .ini files	/etc/php5/conf.d
Additional .ini files parsed	/etc/php5/conf.d/ctype.ini, /etc/php5/conf.d/dom.ini, /etc/php5/conf.d/gd.ini, /etc/php5/conf.d/gettext.ini, /etc/php5/conf.d/iconv.ini, /etc/php5/conf.d/json.ini, /etc/php5/conf.d/mbstring.ini, /etc/php5/conf.d/mysql.ini, /etc/php5/conf.d/mysqli.ini, /etc/php5/conf.d/pdo.ini, /etc/php5/conf.d/pdo_mysql.ini, /etc/php5/conf.d/pdo_sqlite.ini, /etc/php5/conf.d/php.ini, /etc/php5/conf.d/sqlite3.ini, /etc/php5/conf.d/suhosin.ini, /etc/php5/conf.d/tokenizer.ini, /etc/php5/conf.d/xmlreader.ini, /etc/php5/conf.d/xmlwriter.ini, /etc/php5/conf.d/zlib.ini
PHP API	20121113
PHP Extension	20121212
Zend Extension	220121212
Zend Extension Build	API220121212,NTS
PHP Extension Build	API20121212,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring

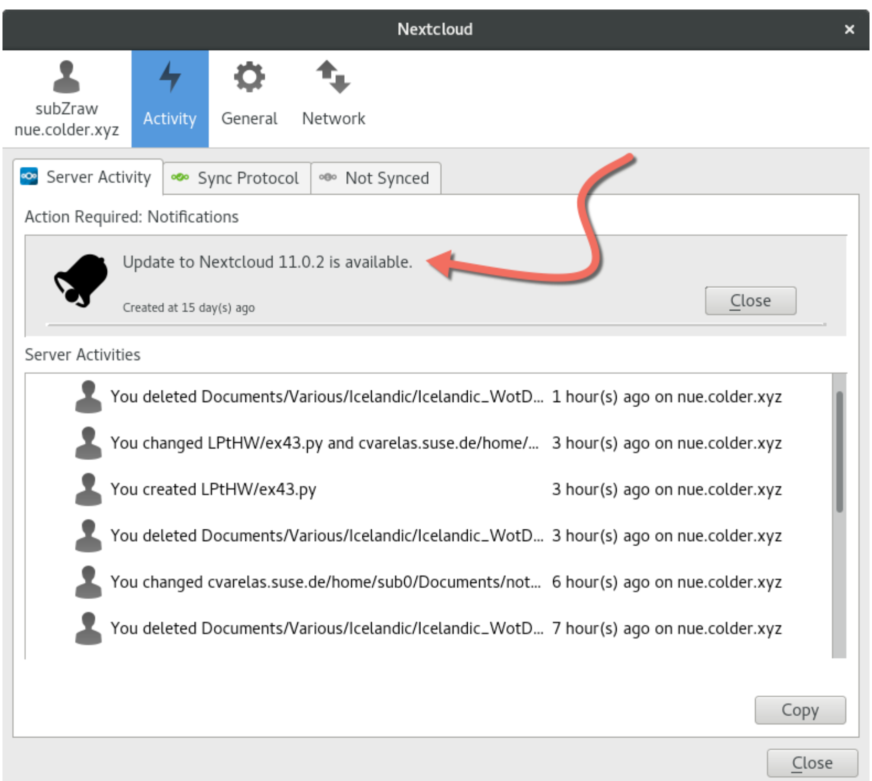
O nginx είναι πλέον ικανός να μεταχειρίζεται αρχεία PHP χάρη στο php-fpm – κι εμείς έχουμε ένα πλήρες LEMP stack στον openSUSE server μας. Παρεμπιπτόντως, το αρχείο info.php που δημιουργήσαμε πριν λίγο δεν το χρειαζόμαστε άλλο και τώρα μπορούμε να το διαγράψουμε.

Skill: Beginner
Tags: Nextcloud, administration

Αναβάθμιση Nextcloud από το web panel

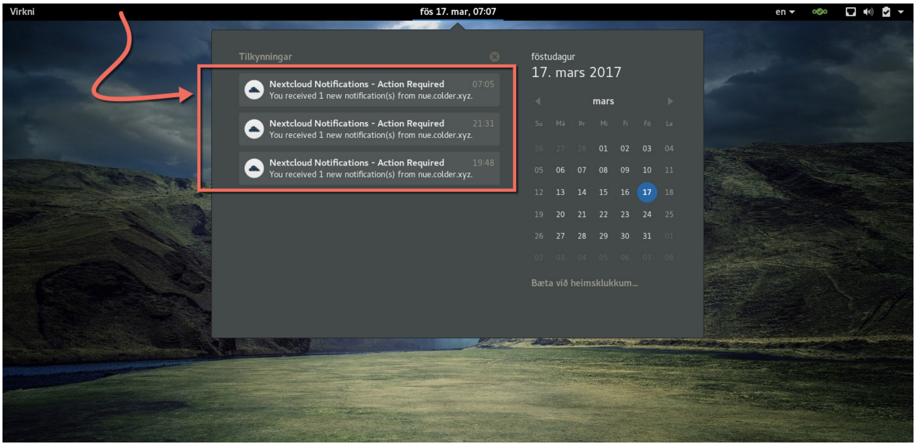
Όταν φτάνει η ώρα για την αναβάθμιση του Nextcloud, το σύστημα δεν χάνει ευκαιρία για να μας το θυμίζει. Όσο φασαριόζικη κι αν φαντάζει μια τέτοια δουλειά καλό είναι να μην την αμελούμε — ειδικά αν ο server είναι προσβάσιμος από το Internet.

Ευτυχώς η όλη διαδικασία επιτυγχάνεται εύκολα, μέσα από το web panel του Nextcloud. Όταν λοιπόν υπάρχει διαθέσιμη αναβάθμιση, το πληροφορούμαστε με ένα σωρό τρόπους. Δείτε, π.χ., τα τρία screenshots που ακολουθούν.

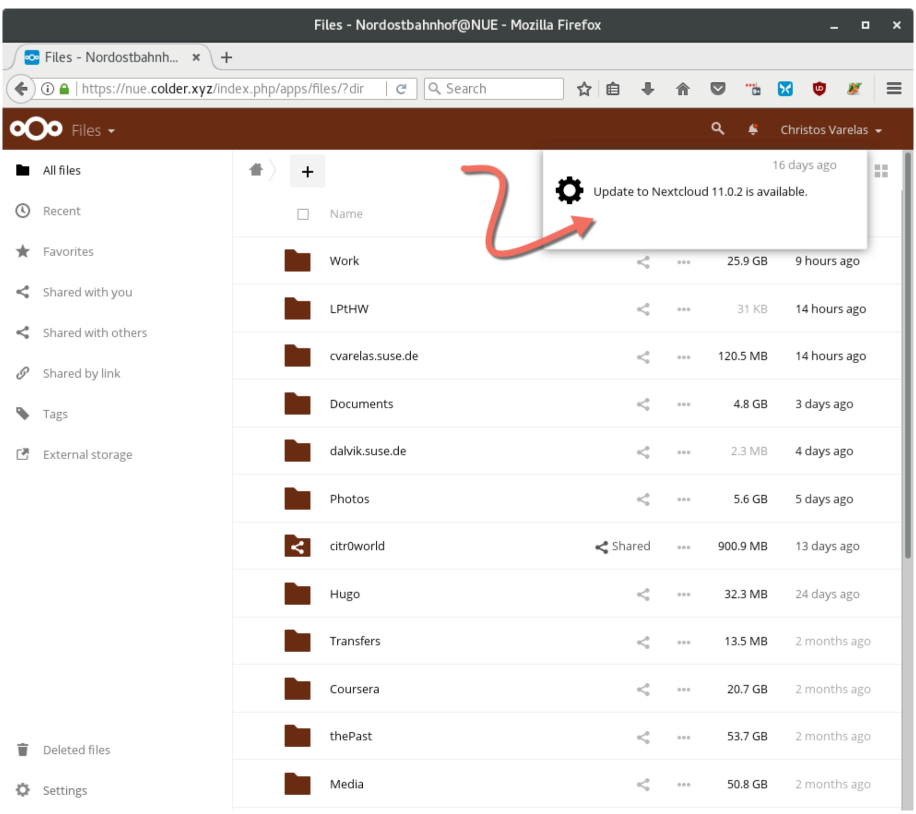


Μας αρέσει ο επίσημος client για το Nextcloud (https://nextcloud.com/install/#install-clients), ο οποίος διατίθεται για όλα τα γνωστά desktop operating systems. Στο στιγμιότυπο απεικονίζεται η εκδοχή για Linux και, όπως βλέπετε, ενημερώνει για τη νέα έκδοση του Nextcloud (την 11.0.2).

Αναβάθμιση Nextcloud από το web panel

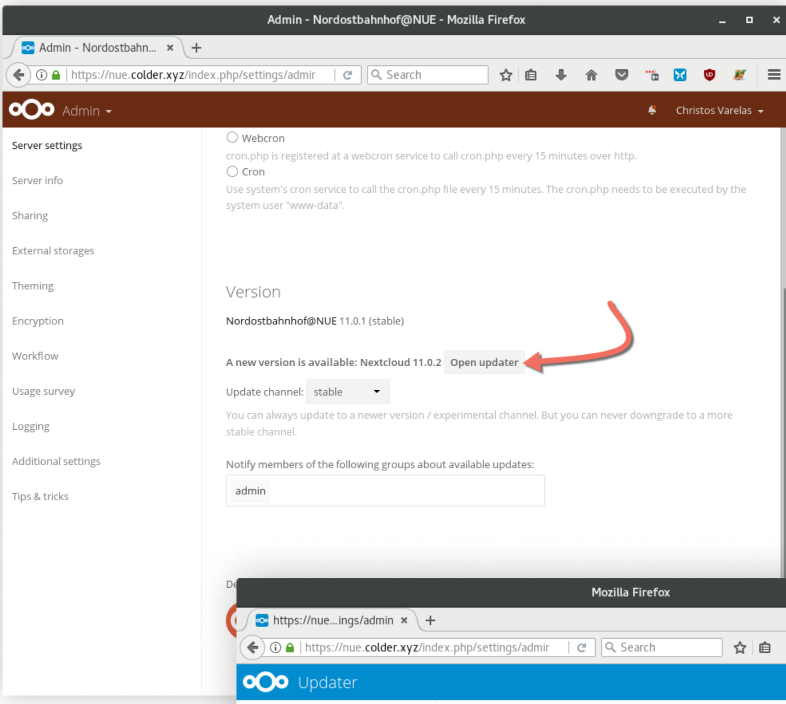


Ειδοποιήσεις για τη διαθεσιμότητα νέας έκδοσης εμφανίζει και το περιβάλλον του GNOME.

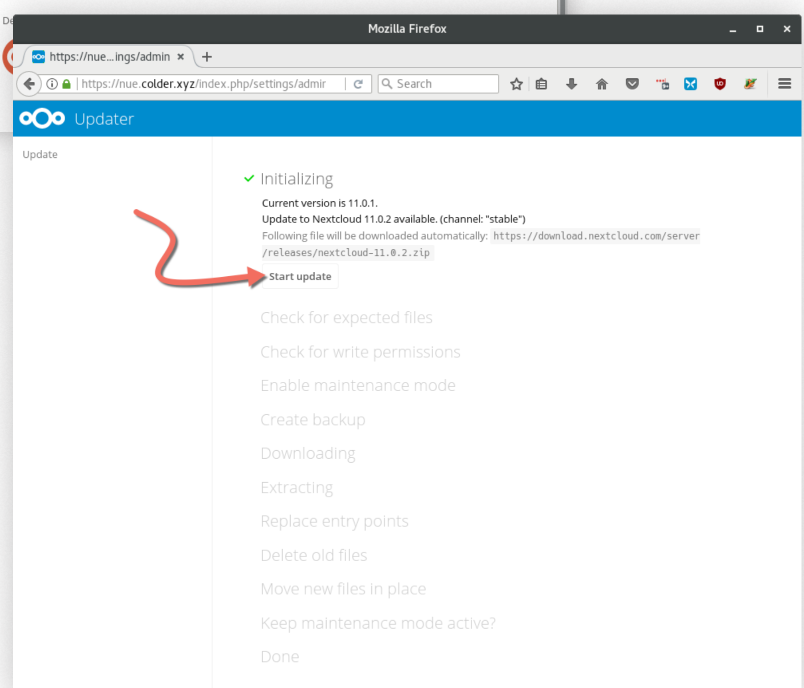


Ακόμη κι αν δεν χρησιμοποιούμε κάποιον client για το Nextcloud, με login στο web panel της πλατφόρμας παίρνουμε ειδοποίηση για τη νέα διαθέσιμη έκδοση.

Προκειμένου ν' αναβαθμίσουμε το Nextcloud με χρήση του παρεχόμενου web panel, από τον browser της προτίμησής μας συνδεόμαστε σε έναν λογαριασμό της πλατφόρμας ο οποίος έχει δικαιώματα διαχειριστή. Κάνουμε ένα κλικ στο όνομα του αντίστοιχου χρήστη (πάνω δεξιά) κι επιλέγουμε το Admin. Στη νέα σελίδα που εμφανίζεται, πατάμε στο κουμπί Open updater.



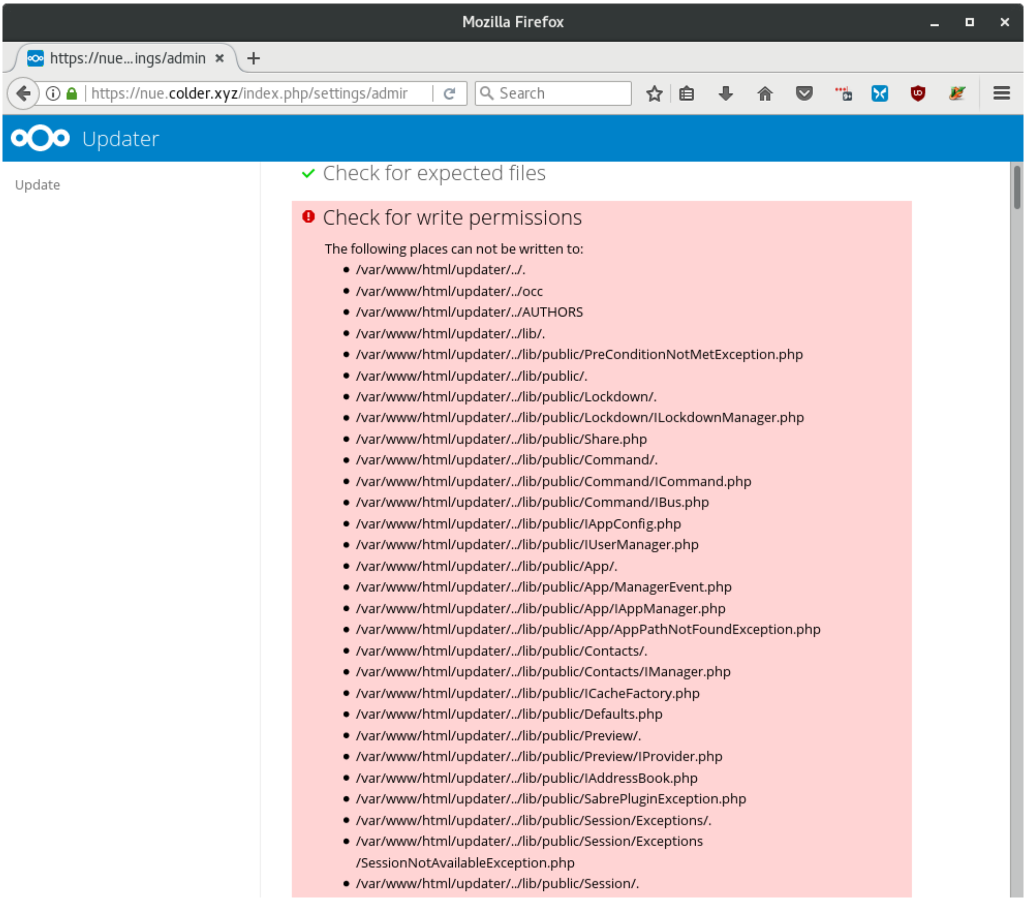
Στη σελίδα Admin, στο web panel του Nextcloud, φτάνουμε έχοντας πρώτα κάνει login σε λογαριασμό χρήστη με δικαιώματα διαχειριστή. Η διαδικασία της αναβάθμισης ξεκινά με κλικ στο κουμπί Open updater.



Στη νέα σελίδα που εμφανίζεται βλέπουμε την τρέχουσα έκδοση του Nextcloud, καθώς κι αυτή στην οποία θα βρισκόμαστε μετά την αναβάθμιση. Προχωράμε με κλικ στο Start update.

Αναβάθμιση Nextcloud από το web panel

Αναλόγως των αδειών πρόσβασης στον κατάλογο όπου είναι εγκατεστημένο το Nextcloud, η διαδικασία της αναβάθμισης είναι πολύ πιθανό να σταματήσει πρόωρα και στον browser να εμφανιστεί μήνυμα για έλεγχο των δικαιωμάτων για εγγραφή.

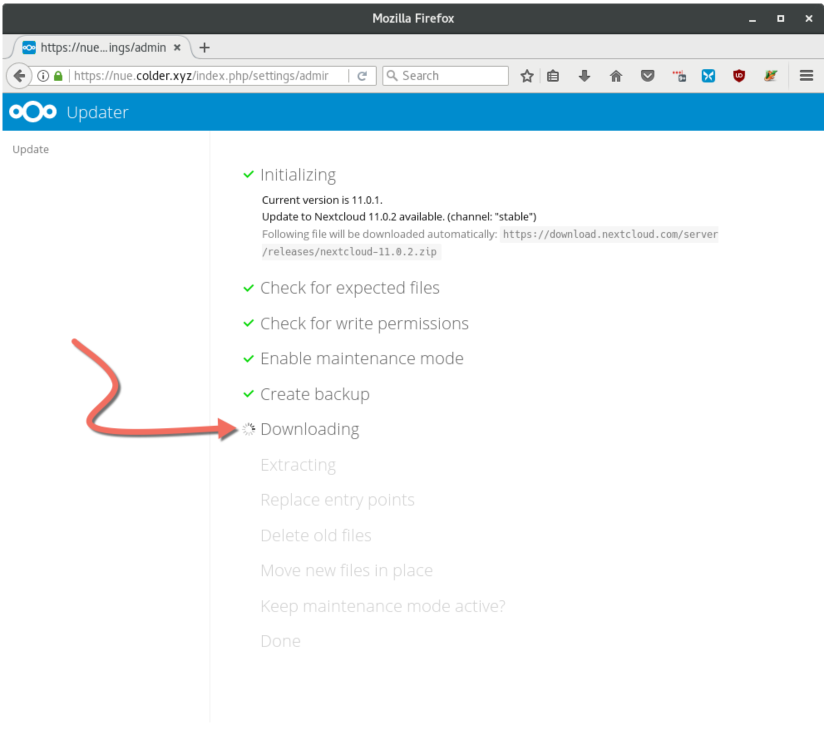


Η αναβάθμιση δεν μπορεί να προχωρήσει, αφού δεν επιτρέπεται η εγγραφή εντός του καταλόγου όπου βρίσκεται το Nextcloud :/

Στο πλαίσιο του παραδείγματός μας αναβαθμίζουμε μια εγκατάσταση του Nextcloud σε Raspberry Pi (βλ. άρθρο σελ. 14). Η πλατφόρμα βρίσκεται εντός του /var/www/html κι ο κατάλογος ανήκει στο χρήστη με username το pi, ο οποίος είναι κι ο μόνος με δικαιώματα εγγραφής. Μεταξύ των περιεχομένων του html υπάρχουν δύο υποκατάλογοι, οι apps και config, οι οποίοι ανήκουν στο χρήστη www-data. Μέσα από τον ομώνυμο λογαριασμό τρέχει ο updater του Nextcloud και, κατά πώς φαίνεται, χρειάζεται δικαιώματα εγγραφής και σ' άλλους καταλόγους. Αφού σημειώσαμε τους υποκαταλόγους του html που ανήκουν στον www-data, δώσαμε στον εν λόγω χρήστη το ιδιοκτησιακό καθεστώς του καταλόγου /var/www/html καθώς και *όλων* των περιεχομένων του:

```
pi@nordostbahnhof:~ $ sudo chown -R www-data:www-data /var/www/html
```

Μετά ξεκινήσαμε και πάλι την εγκατάσταση του Nextcloud, κι αυτή τη φορά η διαδικασία προχώρησε ομαλά.

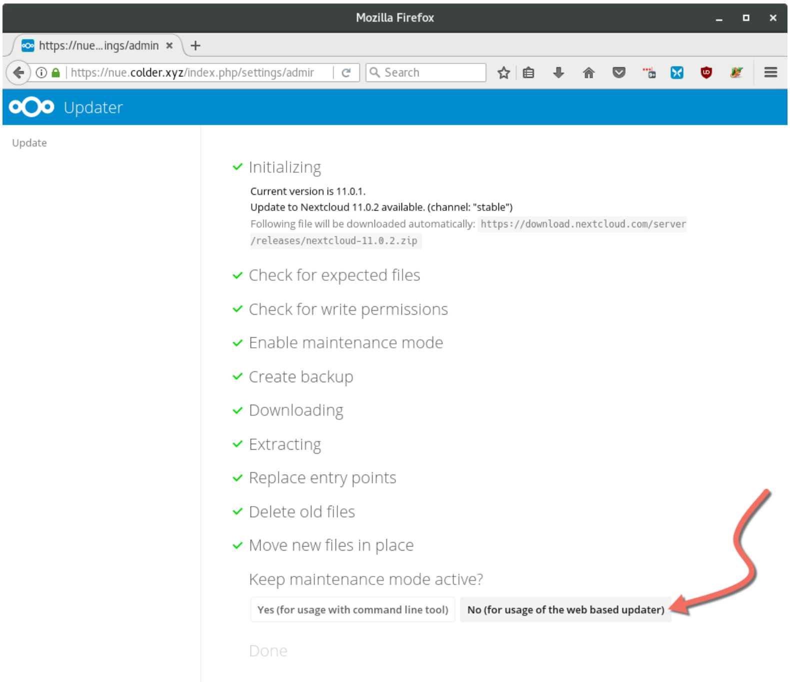


Αφού δώσαμε στο χρήστη www-data το ιδιοκτησιακό καθεστώς του καταλόγου /var/www/html, επιχειρήσαμε και πάλι την αναβάθμιση κι αυτή τη φορά η διαδικασία προχώρησε ομαλά.

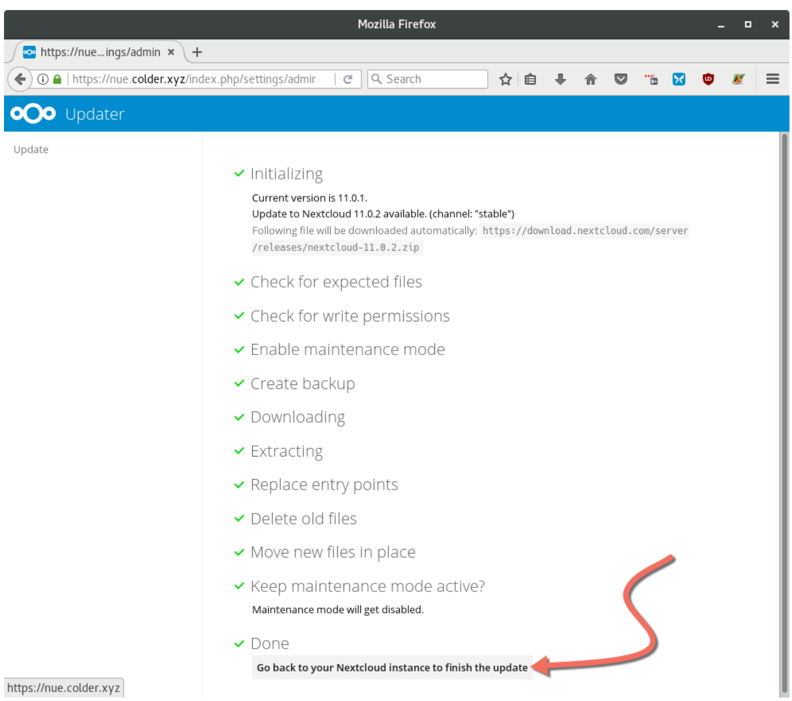
Παρακολουθήστε στα screenshots που ακολουθούν πώς ολοκληρώνεται η αναβάθμιση του Nextcloud. Μετά το πέρας της, μην ξεχάσετε να επαναφέρετε το ιδιοκτησιακό καθεστώς του καταλόγου /var/www/html στην πρότερη κατάσταση. Εμείς, π.χ., στο Raspberry Pi πληκτρολογήσαμε τα ακόλουθα:

```
pi@nordostbahnhof:~ $ sudo chown -R pi:pi /var/www/html
pi@nordostbahnhof:~ $ sudo chown -R www-data:www-data /var/www/html/apps
pi@nordostbahnhof:~ $ sudo chown -R www-data:www-data /var/www/html/config
```

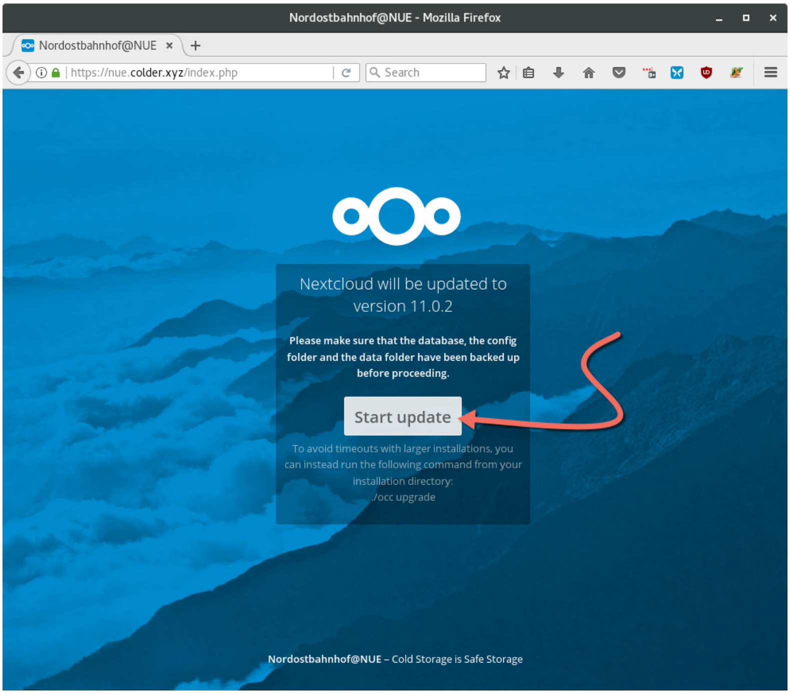
Αναβάθμιση Nextcloud από το web panel



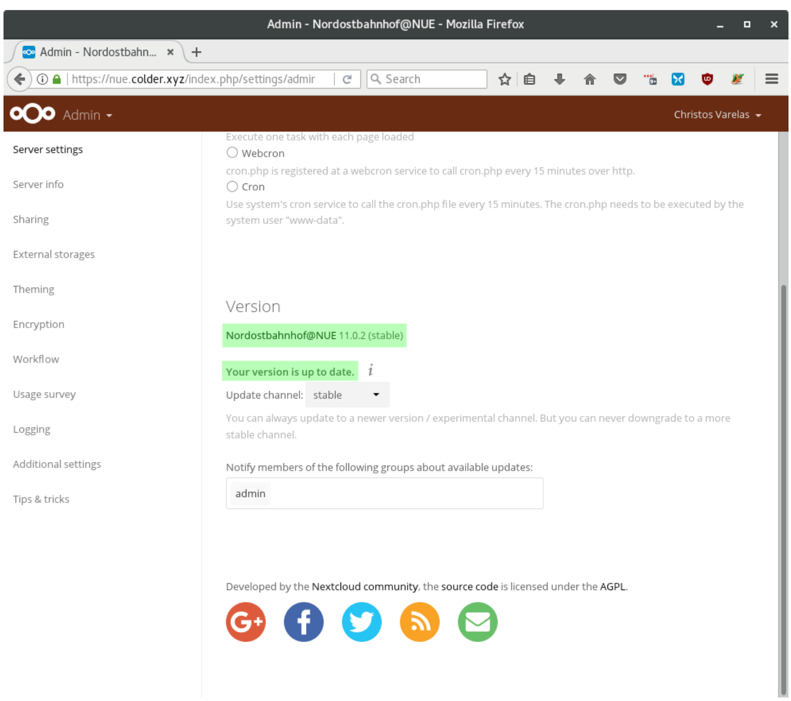
Κατά την αναβάθμιση το Nextcloud μπαίνει σε maintenance mode. Θα ολοκληρώσουμε τη διαδικασία με τη βοήθεια του web based updater κι όχι από τη γραμμή εντολών, οπότε τώρα κάνουμε κλικ στο κουμπί No (for usage of the web based updater) κάτω δεξιά.



Μετά την επιλογή του web updater πατάμε στο κουμπί στο κάτω μέρος της σελίδας, ώστε να τελειώσουμε με την αναβάθμιση.



Μεταφερόμαστε ξανά στην αρχική σελίδα του Nextcloud. Ακόμη δεν βλέπουμε τη συνηθισμένη προτροπή για login σε λογαριασμό χρήστη, ούτε τους καταλόγους και τα αρχεία κάποιου υπάρχοντα χρήστη. Αντίθετα, καλούμαστε να πατήσουμε το κουμπί Start update. Αναλόγως του μεγέθους της εγκατάστασης, το τελευταίο αυτό στάδιο ίσως διαρκέσει αρκετά λεπτά.



Η αναβάθμιση ολοκληρώθηκε επιτυχώς. Έχουμε, πλέον, την πιο πρόσφατη έκδοση του Nextcloud (από το κανάλι Stable).

Skill: Intermediate
Tags: macOS, virtual networks, name servers, DNS resolution

Φορητά εικονικά εργαστήρια

και ρυθμίσεις δικτύωσης αναλόγως της τοποθεσίας

Για τα laptop που αλλάζουν συχνά φυσική τοποθεσία, κι επομένως συνδέονται συχνά σε διαφορετικά δίκτυα, οι παράμετροι δικτύωσης που λαμβάνονται από τον εκάστοτε router μερικές φορές δεν βολεύουν.

Το λιγότερο που αλλάζει από δίκτυο σε δίκτυο είναι η διεύθυνση IP του laptop, η διεύθυνση του gateway (router), καθώς και οι name servers. Για τις δύο πρώτες παραμέτρους είναι μάλλον απίθανο να νοιαστούμε, ίσως όμως έχουμε ενστάσεις για την τρίτη. Μπορεί, π.χ., να μην εμπιστευόμαστε τους name servers που παρέχονται αυτόματα από τον router μπροστά μας και να θέλουμε να χρησιμοποιήσουμε εκείνους της Google (8.8.8.8 και 8.8.4.4) ή κάποιον (εικονικό) recursive name server που τρέχουμε τοπικά, στον ίδιο μας τον υπολογιστή (για τα διάφορα είδη name servers διαβάστε το σχετικό άρθρο στο https://deltahacker.gr/?p=14739).

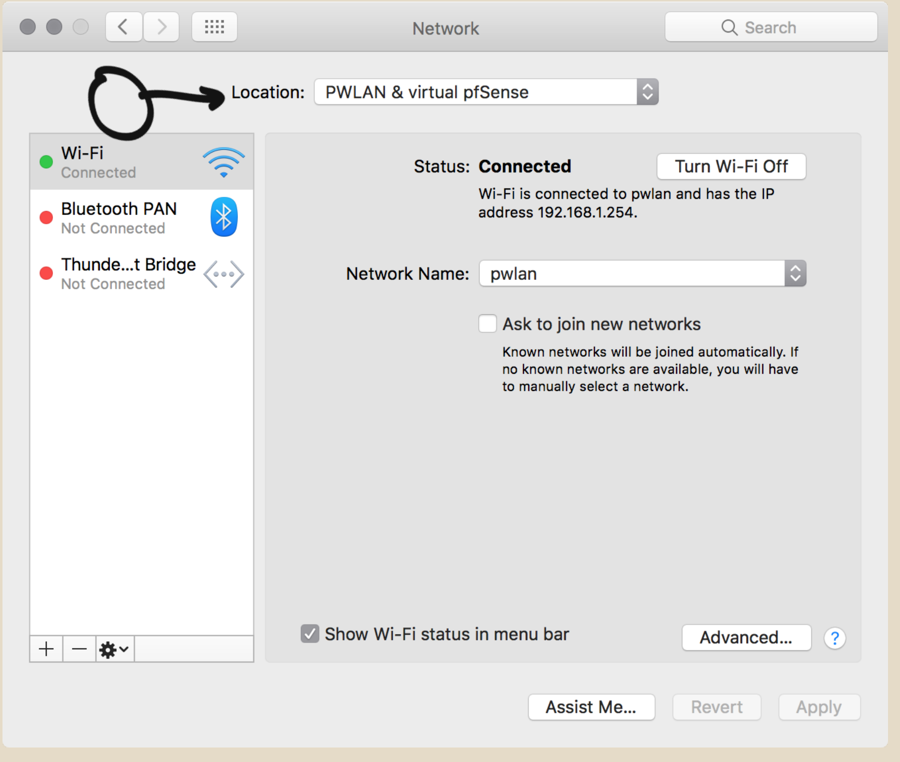
Αλλά το να μη δεχόμαστε πάντοτε τους name servers που γνωστοποιούνται από τον όποιον router και κατά περίπτωση να υποδεικνύουμε τον δικό μας ή τους δικούς μας, δεν έχει πάντα να κάνει με ζητήματα εμπιστοσύνης. Στο MacBook που χρησιμοποιεί ο γράφων, για παράδειγμα, ενίοτε λειτουργεί ένα εικονικό δίκτυο, το οποίο έχει τον δικό του εικονικό router με το θαυμάσιο pfSense (https://deltahacker.gr/?p=8234). Όταν γίνεται χρήση του εικονικού δικτύου, θέλουμε να φτάνουμε στα VMs πίσω από το pfSense πληκτρολογώντας τα FQDNs τους κι όχι τις αντίστοιχες αριθμητικές διευθύνσεις IP. Παράδειγμα: Αντί από το host OS (με το macOS) να συνδεόμαστε σε ένα VM με openSUSE πληκτρολογώντας στο τερματικό `ssh sub0@172.16.164.204`, προτιμάμε να πληκτρολογούμε `ssh sub0@holmavik.colder.local` ή ακόμη και `ssh sub0@holmavik` (όπου holmavik είναι το hostname του VM και colder.local είναι το εσωτερικό domain που εξυπηρετεί το pfSense).

Μία πρώτη λύση σ' αυτό το πρόβλημα είναι να ενημερώσουμε κατάλληλα το αρχείο /etc/hosts του macOS, ώστε να περιλαμβάνει γραμμές της μορφής

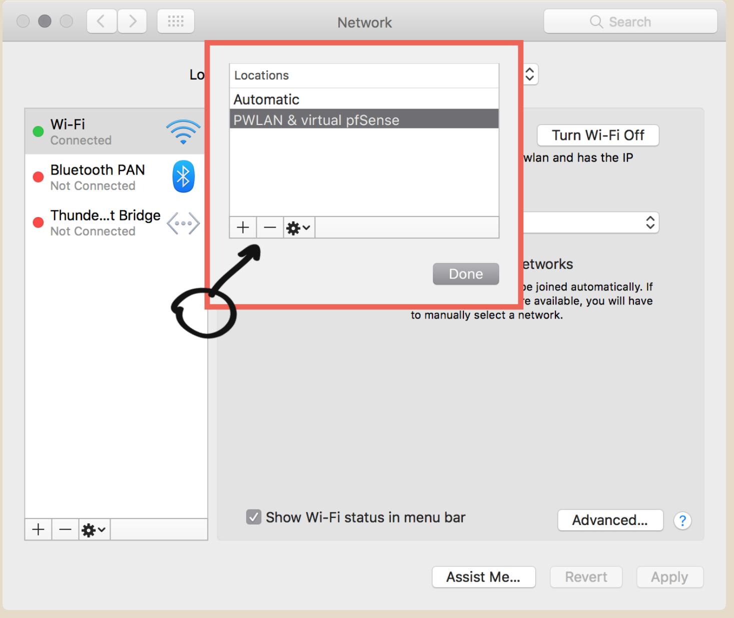
```
172.16.164.204 holmavik holmavik.colder.local
```

Επιπρόσθετα, μπορούμε να ρυθμίσουμε το pfSense ώστε σε συγκεκριμένα VMs να δίνει πάντοτε την ίδια διεύθυνση IP (με βάση το MAC address της αντίστοιχης εικονικής κάρτας δικτύου), ώστε οι σχετικές γραμμές εντός του /etc/hosts να είναι πάντοτε έγκυρες. Ξέρετε κάτι, όμως; Πολλά VMs σήμερα είναι, αύριο δεν είναι. Αυτό σημαίνει ότι οι πληροφορίες εντός του /etc/hosts δύσκολα θα παραμένουν επίκαιρες και συχνά πυκνά θα πρέπει να επεμβαίνουμε.

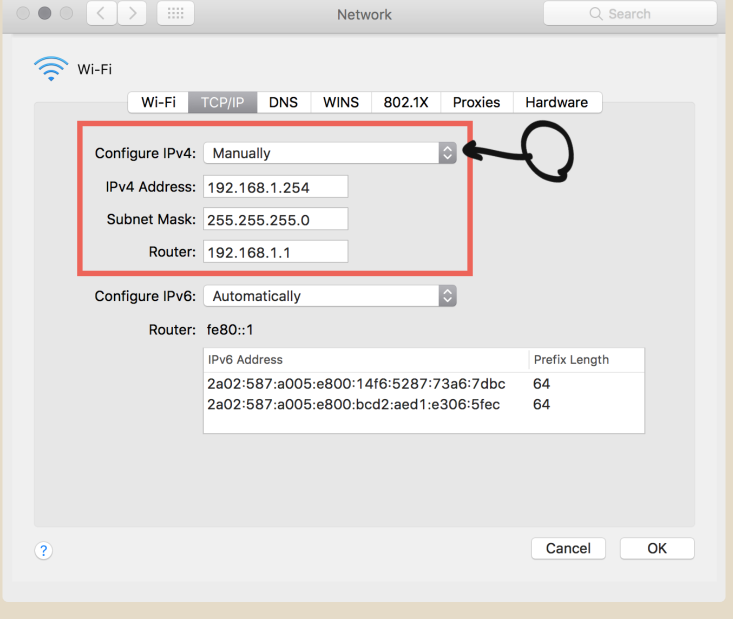
Μια καλύτερη λύση είναι να εκμεταλλευτούμε τα προφίλ σύνδεσης αναλόγως της τοποθεσίας. Η σχετική δυνατότητα παρέχεται σε macOS, Linux και Windows, στο παρόν άρθρο όμως επικεντρωνόμαστε στο πρώτο από τα τρία λειτουργικά. Η γενική ιδέα είναι ότι ναι μεν ο υπολογιστής μας συνδέεται σε ένα ενσύρματο ή ασύρματο δίκτυο και λαμβάνει αυτόματα ρυθμίσεις δικτύωσης από τον router μπροστά του, ανά πάσα στιγμή όμως ενεργοποιούμε ένα από τα προφίλ δικτύωσης που έχουμε δημιουργήσει κι αυτομάτως κάποια πράγματα αλλάζουν και γίνονται όπως ακριβώς μας βολεύει. Για ένα συγκεκριμένο σενάριο, δείτε τα τέσσερα screenshots που ακολουθούν και βεβαίως διαβάστε τις αντίστοιχες περιγραφές.



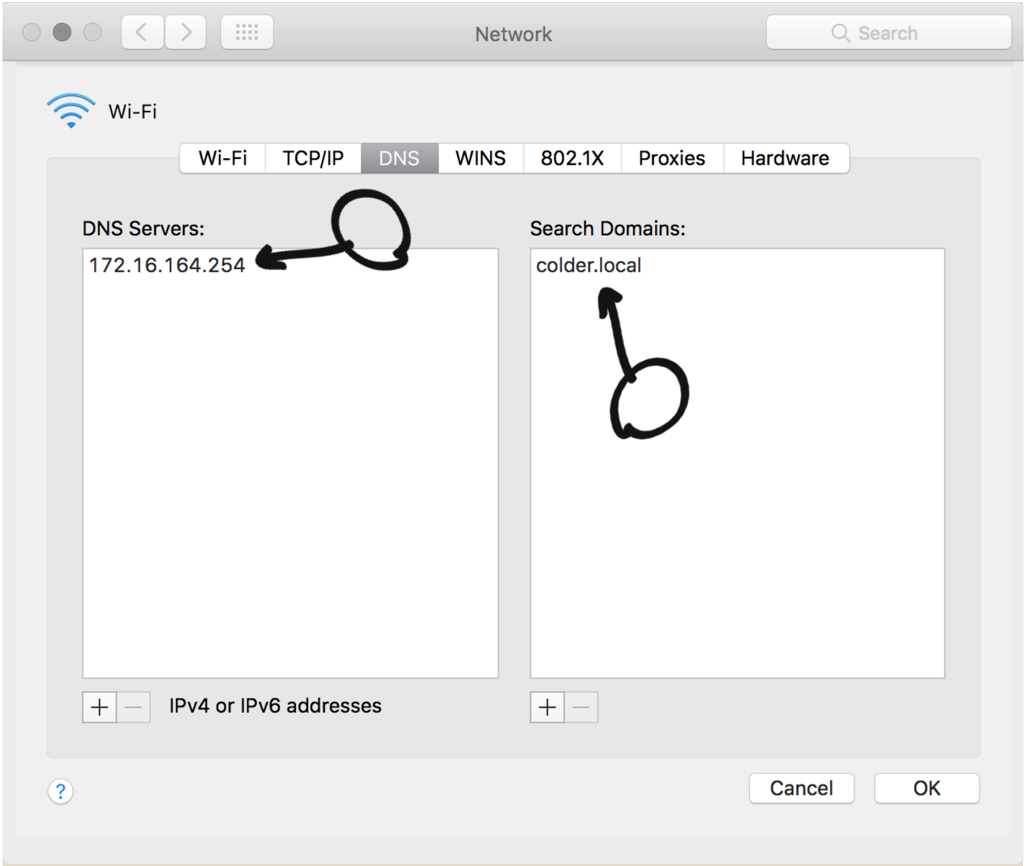
*Είμαστε συνδεδεμένοι ασύρματα σε ένα Access Point με όνομα pwlan, όπως βλέπετε όμως αντί για το location ονόματι "Automatic" έχουμε επιλέξει ένα άλλο, με όνομα "PWLAN & virtual pfSense". Αν είχαμε αφήσει την τοποθεσία Automatic, το laptop θα λάμβανε όλες *ανεξαιρέτως* τις παραμέτρους δικτύωσης από τον αντίστοιχο ασύρματο router. Στη συγκεκριμένη περίπτωση αυτό καθόλου δεν μας πειράζει, αφού εμπιστευόμαστε απόλυτα το δίκτυο (είναι στο σπίτι των γονέων και τον router τον έχουμε ρυθμίσει εμείς οι ίδιοι). Από το όνομα του επιλεγμένου location, όμως, είναι φανερό ότι η παρουσία του (εικονικού) pfSense router αλλάζει κάπως το σκηνικό της δικτύωσης.*



Με κλικ στο drop-down μενού στα δεξιά του Location, εκτός από την επιλογή υπάρχουσας τοποθεσίας έχουμε τη δυνατότητα να ορίζουμε νέες ή να διαγράφουμε παλιές (πατήστε στο Edit Locations). Προκειμένου να υποδείξουμε τις παραμέτρους δικτύωσης για μια συγκεκριμένη τοποθεσία αρχικά την επιλέγουμε, κάνουμε ένα κλικ στο κουμπί Apply, κάτω δεξιά, μετά πατάμε και στο κουμπί Advanced από πάνω.



Έχουμε επιλεγμένη την τοποθεσία "PWLAN & virtual pfSense" και παρατηρούμε τις αντίστοιχες ρυθμίσεις δικτύωσης. Στην καρτέλα TCP/IP, δείτε ότι για το Configure IPv4 υπάρχει το Manually. Έχουμε ρυθμίσει εμείς οι ίδιοι τον συγκεκριμένο wireless router κι έτσι γνωρίζουμε τη διεύθυνσή του (192.168.1.1), καθώς κι ότι το 192.168.1.254 είναι εκτός του εύρους διευθύνσεων που μοιράζει ο αντίστοιχος DHCP server. Αν πάλι δεν γνωρίζαμε πολλά για τον wireless router, για το Configure IPv4 κάλλιστα θα μπορούσαμε να είχαμε αφήσει το Using DHCP (και συνεπώς τα IPv4 Address, Subnet Mask και Router θα ρυθμίζονταν αυτόματα). Σε κάθε περίπτωση, αυτό που είναι σημαντικό στην περίπτωσή μας είναι να οριστεί από εμάς, δηλαδή όχι αυτόματα, ο name server για τη συγκεκριμένη τοποθεσία.



Ιδού λοιπόν η κρίσιμη παρέμβασή μας, αναφορικά με το DNS. Δείτε ότι έχουμε ορίσει εμείς οι ίδιοι την αριθμητική διεύθυνση IP του μοναδικού name server που θέλουμε (172.16.164.254): πρόκειται για τη διεύθυνση που έχει το LAN interface του εικονικού pfSense router. Επίσης, στο Search Domains έχουμε το colder.local, αφού αυτό είναι το όνομα του εσωτερικού domain που εξυπηρετεί ο recursive name server του pfSense.

deltahacker.gr